

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

University of California Student
Association,

Plaintiff,

v.

Denise Carter, in her official
capacity as Acting Secretary of
Education, et al.,

Defendants.

Civil Action No. 25-354 (RDM)

PLAINTIFF’S MOTION FOR A TEMPORARY RESTRAINING ORDER

Pursuant to Local Civil Rule 65.1(a), Plaintiff University of California Student Association hereby moves for a temporary restraining order, to remain in effect until such time as the Court can further consider the merits of Plaintiff’s claims, enjoining Defendants Acting Secretary of Education Denise Carter and the Department of Education from disclosing information about individuals to individuals affiliated with the so-called Department of Government Efficiency (DOGE), and enjoining Defendants to retrieve and safeguard any such information that has already been obtained by and shared or transferred by DOGE or individuals associated with it.

As set forth in more detail in the accompanying memorandum, Defendants have granted access to records and information about individuals to unauthorized parties in violation of the Privacy Act of 1974, the Internal Revenue Code, and Department of Education regulations. Defendants’ action should be enjoined under the Administrative Procedure Act because it is contrary to law, arbitrary and

capricious, and in excess of Defendants' statutory authority. Plaintiff will suffer imminent and irreparable injury should unlawful access be permitted to continue.

Pursuant to Local Civil Rule 65.1(a), at approximately 8:00 a.m. on February 10, 2025, Plaintiff's counsel emailed the three Assistant Directors for the Federal Programs Branch of the Department of Justice and the Chief of the Civil Division of the U.S. Attorney's Office in D.C. to provide them with electronic copies of the complaint, motion for a temporary restraining order, and accompanying memorandum, declarations, and proposed order via e-mail before completing this electronic filing.

Dated: February 10, 2025

Respectfully submitted,

/s/ Adam R. Pulver

Adam R. Pulver (DC Bar #1020475)
Nandan M. Joshi (DC Bar # 456750)
Public Citizen Litigation Group
1600 20th Street NW
Washington, DC 20009
(202) 588-1000
apulver@citizen.org

Daniel A. Zibel (DC Bar No. 491377)
Alexander S. Elson (DC Bar No. 1602459)
Tyler S. Ritchie
(DC Bar No. 90018119)
National Student Legal Defense Network
1701 Rhode Island Ave. NW
Washington, DC 20036
(202) 734-7495

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

University of California Student
Association,

Plaintiff,

v.

Denise Carter, in her official
capacity as Acting Secretary of
Education, et al.,

Defendants.

Civil Action No. 25-354 (RDM)

**MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR A
TEMPORARY RESTRAINING ORDER**

Daniel A. Zibel
(DC Bar No. 491377)
Alexander S. Elson
(DC Bar No. 1602459)
Tyler S. Ritchie
(DC Bar No. 90018119)
National Student Legal Defense Network
1701 Rhode Island Ave. NW
Washington, DC 20036
(202) 734-7495

Adam R. Pulver
(DC Bar No. 1020475)
Nandan M. Joshi
(DC Bar No. 456750)
Public Citizen Litigation Group
1600 20th Street NW
Washington, DC 20009
(202) 588-1000
apulver@citizen.org

Dated: February 10, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTRODUCTION 1

BACKGROUND 3

 Statutory and Regulatory Framework 3

 ED’s Record Systems 8

 DOGE and DOGE’s access to ED’s systems 13

LEGAL STANDARD 18

ARGUMENT 19

I. Plaintiff has standing 19

 A. Plaintiff’s members are suffering, and will continue to suffer, harm caused by Defendants’ actions and which is redressable by the relief sought 19

 B. The other requirements of associational standing are satisfied 23

II. Plaintiff is likely to succeed on the merits. 24

 A. Defendants’ action giving DOGE access to ED’s records is contrary to law and in excess of their statutory authority 24

 B. Defendants’ action is arbitrary and capricious. 28

III. Plaintiff will suffer immediate, irreparable injury if Defendants continue to allow unlawful access to the EDs records on individuals 29

IV. The balance of equities and the public interest support grant of a TRO 32

CONCLUSION 33

TABLE OF AUTHORITIES

CASES

Advocates for Highway and Auto Safety v. FMCSA,
41 F.4th 586 (D.C. Cir. 2022)..... 19

Ahmed v. Blinken,
No. CV 24-153 (LLA), 2024 WL 4903771 (D.D.C. Nov. 27, 2024) 21

Al-Aulaqi v. Obama,
727 F. Supp. 2d 1 (D.D.C. 2010) 22

Armstrong v. Executive Office of the President,
90 F.3d 553 (D.C. Cir. 1996) 27

Beattie v. Barnhart,
663 F. Supp. 2d 5 (D.D.C. 2009) 30

C.G.B. v. Wolf,
464 F. Supp. 3d 174 (D.D.C. 2020) 33

Cause of Action v. IRS,
125 F. Supp. 3d 145 (D.D.C. 2015) 31

Chaplaincy of Full Gospel Churches v. England,
454 F.3d 290 (D.C. Cir. 2006) 18

Chrysler Corp. v. Brown,
441 U.S. 281 (1979) 25

Church of Scientology of California v. IRS,
484 U.S. 9 (1987) 31

Council on American-Islamic Relations v. Gaubatz,
667 F. Supp. 2d 67 (D.D.C. 2009) 31

Center for Biological Diversity v. EPA,
56 F.4th 55 (D.C. Cir. 2022)..... 20

Center for Biological Diversity v. Regan,
734 F. Supp. 3d 1 (D.D.C. 2024) 20

Center for Biological Diversity v. Trump,
453 F. Supp. 3d 11 (D.D.C. 2020) 25

D.A.M. v. Barr,
474 F. Supp. 3d 45 (D.D.C. 2020) 18

Department of Homeland Security v. Regents of the University of California,
591 U.S. 1 (2020) 29

Doe v. Stephens,
851 F.2d 1457 (D.C. Cir. 1988) 28

*Electronic Privacy Information Center v. National Security Commission on Artificial
Intelligence*,
466 F. Supp. 3d 100 (D.D.C. 2020) 27

*Electronic Privacy Information Center v. Presidential Advisory Commission on
Election Integrity*,
878 F.3d 371 (D.C. Cir. 2017) 19

FAA v. Cooper,
566 U.S. 284 (2012) 32

Hall v. Johnson,
559 F. Supp. 2d 1 (D.D.C. 2009) 18

Hancock v. Urban Outfitters, Inc.,
830 F.3d 511 (D.C. Cir. 2016) 22

Hospitality Staffing Solutions, LLC v. Reyes,
736 F. Supp. 2d 192 (D.D.C. 2010) 31

Hotel & Restaurant Employees Union, Local 25 v. Smith,
846 F.2d 1499 (D.C. Cir. 1988) 19

Magruder v. Capital One, N.A.,
540 F. Supp. 3d 1 (D.D.C. 2021) 22

Medical Imaging & Technology Alliance v. Library of Congress,
103 F.4th 830 (D.C. Cir. 2024)..... 25

Michigan v. EPA,
576 U.S. 743 (2015) 29

*Motor Vehicle Manufacturers Ass’n of United States, Inc. v. State Farm
Mutual Automobile Insurance Co.*,
463 U.S. 29 (1983) 29

NAACP v. Trump,
298 F. Supp. 3d 209 (D.D.C. 2018) 19

National Treasury Employees Union v. U.S. Department of Treasury,
838 F. Supp. 631 (D.D.C. 1993) 31

NB ex rel. Peacock v. District of Columbia,
682 F.3d 77 (D.C. Cir. 2012) 19

**New York v. Trump*,
No. 25 Civ. 1144 (JAV), 2025 WL 435411 (S.D.N.Y. Feb. 8, 2025) 21, 30

Nguyen v. U.S. Department of Homeland Security,
460 F. Supp. 3d 270 (D.D.C. 2020) 19

NRDC v. Raimondo,
No. CV 23-982 (BAH), 2024 WL 4056653 (D.D.C. Sept. 5, 2024) 23

**In re OPM Data Security Breach Litigation*,
928 F.3d 42 (D.C. Cir. 2019) 21, 22

Open Communities Alliance v. Carson,
286 F. Supp. 3d 148 (D.D.C. 2017) 33, 34

Powder River Basin Resource Council v. U.S. Department of Interior,
No. 22-CV-2696 (TSC), 2024 WL 4188655 (D.D.C. Sept. 13, 2024) 24

Pursuing America’s Greatness v. FEC,
831 F.3d 500 (D.C. Cir. 2016) 18

Thompson v. Trump,
590 F. Supp. 3d 46 (D.D.C. 2022) 21

Stark v. Wickard,
321 U.S. 288 (1944) 25

Venetian Casino Resort, LLC v. EEOC,
530 F.3d 925 (D.C. Cir. 2008) 24

Wilcox v. Bastiste,
No. 2:17-cv-122, 2017 WL 2525309, at *3 (E.D. Wash. 2017) 32

STATUTES

Privacy Act of 1974

Pub. L. No. 93-579, 88 Stat. 1896 3

5 U.S.C. § 552a 2

5 U.S.C. § 552a(a)(4) 25

5 U.S.C. § 552a(a)(7) 4

5 U.S.C. § 552a(b)..... 4

*5 U.S.C. § 552a(b)(1)..... 4, 26, 27

5 U.S.C. § 552a(b)(3) 5

5 U.S.C. § 552a(e)(4)..... 4

5 U.S.C. § 552a(e)(10)..... 30

5 U.S.C. § 552a(e)(11)..... 4

5 U.S.C. § 706(2) 24, 25

* 5 U.S.C. § 3161 26

18 U.S.C. § 202(a) 14

Higher Education Act

20 U.S.C. §§ 1070–1099d 1

* 20 U.S.C. § 1090(a)(1) 7, 20

20 U.S.C. § 1090(a)(2)(B) 7

* 20 U.S.C. § 1090(a)(3)(E) 7

* 20 U.S.C. § 1098h(a)(1) 7, 20

Internal Revenue Code

26 U.S.C. § 6103 2, 28

* 26 U.S.C. § 6103(a)..... 5

26 U.S.C. § 6103(b)(1) 5

26 U.S.C. § 6103(b)(2)(A) 5

26 U.S.C. § 6103(b)(6) 5

* 26 U.S.C. § 6103(l)(13) 6, 28

26 U.S.C. § 6103(l)(13)(A) 6

26 U.S.C. § 6103(l)(13)(B) 6

26 U.S.C. § 6103(l)(13)(C) 6

26 U.S.C. § 6103(l)(13)(D)..... 6

26 U.S.C. § 6103(l)(13)(E) 6

26 U.S.C. § 6103(p)(4)(C) 7

26 U.S.C. § 7213A(a) 5

* 31 U.S.C. § 1535(a)..... 26

REGULATIONS

34 C.F.R. § 5b.3 29

34 C.F.R. § 5b.9(b) 5, 29

34 C.F.R. Part 5b, App’x 5

34 C.F.R. § 668.2(b)..... 8

OTHER FEDERAL REGISTER PUBLICATIONS

Executive Order 14158 of January 20, 2025, Establishing and Implementing the President’s “Department of Government Efficiency,”
90 Fed. Reg. 8441 (Jan. 29, 2025)..... 13, 14, 25, 26, 27

Federal Student Aid, U.S. Department of Education, Notice of a modified system of records, Privacy Act of 1974; System of Records,
89 Fed. Reg. 44652 (May 21, 2024)..... 9

Federal Student Aid, U.S. Department of Education, Notice of a new system of records, Privacy Act of 1974; System of Records,
88 Fed. Reg. 42220 (June 29, 2023)..... 11, 12, 28

Federal Student Aid, U.S. Department of Education, Notice of a modified system of records, Privacy Act of 1974; System of Records,
88 Fed. Reg. 41942 (June 28, 2023)..... 9, 10, 28

Federal Student Aid, U.S. Department of Education, Notice of a New System of Records, Privacy Act of 1974; System of Records—Financial Management System (FMS),
73 Fed. Reg. 177 (Jan. 2, 2008)..... 12, 13, 28

OTHER

* Transcript, Press Conference: Donald Trump and Shigeru Ishiba of Japan Hold a Press Event, February 7, 2025 2, 27, 29, 33

Federal Student Aid, U.S. Department of Education, NSLDS, Frequently Asked Questions (FAQs) 8

Collin Binkley & Bianca Vázquez Toness, *Musk team’s access to student loan systems raises alarm over borrowers’ personal information*, Associated Press (Feb. 7, 2025) 17

Nandita Bose & Steve Holland, *Trump makes Musk, the world's richest man, a ‘special government employee’*, Reuters (Feb. 3, 2025) 14

California Student Aid Commission, CADAA for Mixed-Status Families 19

Danielle Douglas-Gabriel, *Consumer groups sue Trump administration over DOGE access*, Wash. Post (Feb. 7, 2025)..... 17, 18

Tyler Kingkade & Natasha Korecki, *Inside DOGE’s takeover of the Education Department*, NBC News (Feb. 8, 2025) 15, 18, 23

Liam Knox & Jessica Blake, *Is DOGE Digging Around in Student Data?*, Inside Higher Ed (Feb. 8, 2025)..... 23

Laura Meckler, et al., *Trump preps order to dismantle Education Dept. as DOGE probes data*, Wash. Post, (Feb. 3, 2025)..... 16

Joseph Menn, et al., *Treasury was warned DOGE access to payments marked an ‘insider threat’*, Wash. Post, (Feb. 7, 2025)..... 17

Hannah Natanson, et al., *Elon Musk’s DOGE is feeding sensitive federal data into AI to target cuts*, Wash. Post (Feb. 6, 2025) 17

Zachary Schermele, *Students sue Education Department, allege DOGE is accessing private data*, USA Today (Feb. 7, 2025)..... 17

Theodore Schleifer, *Young Aides Emerge as Enforcers in Musk’s Broadside Against Government*, N.Y. Times (Feb. 7, 2025)..... 14, 15

Jeff Stein, et al., *U.S government officials privately warn Musk’s blitz appears illegal*, Wash. Post (Feb. 4, 2025) 16

University of California, *The Facts: Federal Financial Aid for UC Students* (Mar. 2021) 20

University of California, Office of the President, *Memo to Members of the Academic & Student Affairs Committee of the Regents of the University of California, Financial Aid Experience for Students*, Jan. 2025 23

INTRODUCTION

Via its Office of Federal Student Aid (FSA), the Department of Education (ED) administers the federal government’s student aid programs for postsecondary education under Title IV of the Higher Education Act, 20 U.S.C. §§ 1070–1099d. To effectuate this responsibility, ED collects and maintains sensitive personal and financial information about millions of students, their parents, and their spouses—including social security numbers (SSNs), dates of birth, driver’s license numbers, citizenship, dependency status, veteran status, marital status, student loan account information, income and asset information, bank account numbers, and tax return information. ED has recognized the sensitivity of the information it collects and maintains, and has repeatedly committed to preserving its privacy—as required by law.

Until now.

Last week, media reports revealed that ED, in disregard of privacy laws and regulations, gave individuals associated with the so-called “Department of Government Efficiency” (DOGE) blanket access to ED’s records systems. ED did not publicly announce this new policy—what is known is based on media reporting—or attempt to justify it. Rather, ED secretly decided to allow individuals with no role in the federal student aid program to root around millions of students’ sensitive records.

Giving access to those records is unlawful. Congress has enacted laws to assure the public that, when they submit their personal information to the federal government, their information will be protected from improper and unnecessary disclosure to third parties—whether within or outside the government. Two such

laws are implicated here. The Privacy Act of 1974 bars agencies from sharing records about individuals with third parties. 5 U.S.C. § 552a. The Internal Revenue Code is even more protective, requiring personal information related to taxes to be kept “confidential.” 26 U.S.C. § 6103. None of the targeted exceptions in these laws allows individuals associated with DOGE, or anyone else, to obtain or access students’ personal information, except for specific purposes—purposes not implicated here.

Notably, when on February 7, 2025, President Trump was asked by a reporter why DOGE needs access to Americans’ personal information, like social security numbers, home addresses, and bank accounts, President Trump responded, “Well, it doesn’t.”¹ Plaintiff agrees. And thus none of the statutory provisions that allow disclosure based on need are applicable. ED thus should have denied access. Instead, ED opened up its records to provide DOGE with ongoing access to individuals’ personal and financial information.

Plaintiff University of California Student Association (UCSA) is a membership organization of over 230,000 students at the nine campuses of the University of California—more than 70% of whom currently receive federal financial aid. These members have no choice whether to give ED access to their personal and financial information if they want to participate in federal student aid programs—including the Pell Grant, Direct Loan, and work-study program. But by giving DOGE full access

¹ Transcript, Press Conference: Donald Trump and Shigeru Ishiba of Japan Hold a Press Event, February 7, 2025, available at <https://rollcall.com/factbase/trump/transcript/donald-trump-press-conference-shigeru-ishiba-japan-february-7-2025/>.

to ED's systems, Defendants have given unknown individuals access to the personal information of Plaintiff's members without those members' knowledge or consent. That decision has resulted in the infringement of Plaintiff's members' constitutional and statutory privacy rights, has caused them significant emotional distress, and puts them at greater risk of identity theft. These harms are happening right now, because individuals associated with DOGE are already in ED's system and, reportedly, using Plaintiff's members' data. In these circumstances, a temporary restraining order (TRO) is vital to protect the individual privacy of Plaintiff's members until this Court can thoroughly consider and resolve this dispute.

BACKGROUND

Statutory and Regulatory Framework

1. ***Privacy Act.*** Recognizing that “the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies,” Congress enacted the Privacy Act to “regulate the collection, maintenance, use, and dissemination of information by such agencies.” Pub. L. No. 93-579, §2(a)(1), (5), 88 Stat. 1896, 1896 (1974). The Privacy Act provides “safeguards for an individual against an invasion of personal privacy by requiring Federal agencies ... to ... collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose [and] that adequate safeguards are provided to prevent misuse of such information.” *Id.* § 2(b)(4).

Under the Privacy Act, an agency that maintains a system of records about individuals must publish a notice in the Federal Register “of the existence and

character” of that system. 5 U.S.C. § 552a(e)(4). This notice is referred to as a System of Records Notice (SORN). An agency must give the public 30 days’ notice of a new or revised SORN and must provide an opportunity to comment on the proposed SORN. *Id.* § 552a(e)(11). A SORN must disclose, among other things, “the categories of individuals on whom records are maintained in the system,” “the categories of records maintained in the system,” “each routine use of the records contained in the system, including the categories of users and the purpose of such use,” and “the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.” *Id.* § 552a(e)(4). A “routine use” of a record is “the use of such record for a purpose which is compatible with the purpose for which it was collected.” *Id.* § 552a(a)(7).

The Privacy Act also safeguards against disclosure of records. Absent the consent of the individual to whom a particular record pertains, agencies may not disclose a record “to any person, or to another agency.” *Id.* § 552a(b) . The Privacy Act lists 13 exceptions to the bar on disclosure, only two of which appear to be remotely relevant here. First, an agency may disclose the records it maintains within the agency “to those officers and employees of the agency ... who have a need for the record in the performance of their duties.” *Id.* § 552a(b)(1). Second, an agency may disclose a record pursuant to a “routine use” identified in its SORN. *Id.* § 552a(b)(3).

ED’s implementing regulations similarly prohibit the disclosure of individuals’ records without consent except in limited circumstances; the only two regulatory exceptions relevant here mirror the statutory exceptions in sections 552a(b)(1) and

a(b)(3). 34 C.F.R. § 5b.9(b). The regulations also impose Employee Standards of Conduct, which require ED employees to “guard against improper disclosure of records which are governed by the [Privacy] Act,” and impose specific additional obligations to guard against such improper disclosure. 34 C.F.R. Part 5b, App’x.

2. *The Internal Revenue Code.* Congress has enacted heightened protections for information that taxpayers submit in connection with tax filings. Under 26 U.S.C. § 6103(a), “[r]eturns and return information shall be confidential.” A “return” includes “any tax or information return” or “claim for refund.” *Id.* § 6103(b)(1). “Return information” includes “a taxpayer’s identity” and “any other data, received by, recorded by, prepared by, furnished to, or collected” in connection with federal taxes. *Id.* § 6103(b)(2)(A). A taxpayer’s identity is defined to include not just the taxpayer’s name but also mailing address and taxpayer identifying number. *Id.* § 6103(b)(6). Section 6103(a) makes clear that “no officer or employee of the United States” may disclose a return or return information if the disclosure is not expressly authorized. *See also* 26 U.S.C. § 7213A(a) (making it “unlawful” for “any officer or employee of the United States” “to inspect, except as authorized in [title 26], any return or return information”).

Section 6103 lists detailed exceptions to the confidentiality requirement. With respect to ED, section 6103(d)(13) authorizes the Secretary of the Treasury, upon written request from the Secretary of Education, to disclose certain return information to “an authorized person” only:

- “for the purpose of (and to the extent necessary in) determining eligibility for, or repayment obligations under, income-contingent or income-based repayment plans,” 26 U.S.C. § 6103(l)(13)(A);
- “for the purpose of (and to the extent necessary in) monitoring and reinstating loans...that were discharged based on a total and permanent disability,” *id.* § 6103(l)(13)(B); and
- “for the purpose of (and to the extent necessary in) determining eligibility for, and amount of, Federal student financial aid,” *id.* § 6103(l)(13)(C).

The statute permits “an authorized person” to use information provided under these three provisions for “reducing the net cost of improper payments under such plans” and programs, for “oversight activities by the Office of Inspector General of the Department of Education,” and for “conducting analyses and forecasts for estimating costs related to such plans, awards, or discharges,” *id.* § 6103(l)(13)(D)(i)(I)-(III). The statute explicitly prohibits the use of such information for criminal investigations or prosecutions, *id.* § 6103(l)(13)(D)(ii), and authorizes redisclosure only for narrow specific purposes, *id.* § 6103(l)(13)(D)(iii)–(vi).

To be an “authorized person,” an individual must meet two mandatory criteria: (1) they must be an “officer, employee, or contractor of [ED], and (2) they must be “specifically authorized and designated by the Secretary of Education” to use the information for one of the purposes set out in sections 6103(l)(13)(A–C). *Id.* at § 6103(l)(13)(E).

Finally, 26 U.S.C. § 6103(p)(4)(C) requires agencies who receive tax return information pursuant to section 6103(l)(13) and other similar provisions to “restrict ... access to the returns or return information only to persons whose duties or

responsibilities require access and to whom disclosure may be made under the provisions of this title.”

3. *The Student Assistance Programs Statute.* Title 20 of the U.S. Code, at Chapter 28, Subchapter IV, Part G, contains numerous provisions governing ED’s operation of student assistance programs, several of which are particularly relevant here. First, section 1090(a) requires “each individual seeking to apply for Federal financial aid” for post-secondary education to file the “Free Application for Federal Student Aid,” or FAFSA, and to provide personal information in twenty different categories, including, but not limited to, name, contact information, social security number, date of birth, marital status, citizenship status, sex, race or ethnicity, asset information, veteran status, and federal benefits history. 20 U.S.C. §§ 1090(a)(1), (a)(2)(B). Section 1098h further requires applicants, as part of their FAFSA application, to affirmatively acknowledge ED’s authority to access their tax return information, and that of their parents or spouse, in order to be eligible for student aid. *Id.* § 1098h(a)(1).

Section 1090(a)(3)(E) explicitly prohibits the disclosure or redisclosure, including “obtaining, sharing, or discussing,” of an applicant’s FAFSA information that includes tax return information, except in accordance with the procedures set out in 20 U.S.C. § 1098h. That provision, in turn, incorporates the limitations on use and redisclosure in 26 U.S.C. § 6103(l)(13), discussed above, and otherwise requires

written consent for the redisclosure, disclosure, or discussion of information in a FAFSA applicant's Student Aid Report.²

ED's Records Systems

Plaintiff's members' personal information is contained in at least four records systems maintained by ED: the National Student Loan Data System, the Common Origination and Disbursement System, the Future Act System, and the Financial Management System.³

1. National Student Loan Data System (NSLDS)

NSLDS is "the national database of information about loans and grants awarded to students under Title IV of the Higher Education Act (HEA)," which "provides a centralized, integrated view of Title IV loans and grants during their complete life cycle, from aid approval through disbursement, repayment, deferment, delinquency, and closure."⁴ Records stored in NSLDS include, but are not limited to, aid applicant and recipient identifier information (including name, date of birth, contact information, SSN, and driver's license number); demographic information, including citizenship, marital status, veteran status, gender, income and asset information; an applicant's "financial profile" as reported and calculated through

² A Student Aid Report, or SAR, is "a report provided to an applicant by the Secretary showing his or her FAFSA information and the amount of his or her [estimated financial contribution]. 34 C.F.R. § 668.2(b).

³ Plaintiff's members' personal information may be contained within other systems to which DOGE-affiliated individuals have access, but Plaintiff lacks clear information about such access at this time.

⁴ See FSA, NSLDS, Frequently Asked Questions (FAQs), <https://nslsdfap.ed.gov/help/faq>.

FAFSA; information from federal loan applications; and information about applicants' parent(s) or spouses, including their SSNs, contact information, and income and asset information.⁵

The most recent SORN for NSLDS was published on May 21, 2024.⁶ It specifies that “[a]ccess to the system is limited to authorized NSLDS program personnel and contractors responsible for administering the NSLDS program,” and “strictly limit[s]” access to records housed in the system “to those staff members trained in accordance with the Privacy Act and Automatic Data Processing (ADP) security procedures.”⁷ It further identifies particular “routine uses” for which ED may disclose records to specific users.⁸

2. Common Origination and Disbursement System (COD)

COD is a system used to support the origination, disbursement, and reporting for all federal aid programs under Title IV of the Higher Education Act.⁹ It contains records for applicants to, and participants in, any of the Title IV programs including the Pell Grant, Perkins Loan, Academic Competitiveness Grant, National Science and Mathematics Access to Retain Talent Grant, Teacher Education Assistance for College and Higher Education Grant, Iraq and Afghanistan Service Grant, Direct

⁵ FSA, Notice of a modified system of records, Privacy Act of 1974; System of Records, 89 Fed. Reg. 44652, 44656–57 (May 21, 2024).

⁶ *Id.*

⁷ *Id.* at 44660.

⁸ *Id.* at 44657–58.

⁹ FSA, Notice of a modified system of records, Privacy Act of 1974; System of Records, 88 Fed. Reg. 41942, 41942 (June 28, 2023).

Loan, Federal Family Education Loan, Federal Work-Study, and Federal Supplemental Educational Opportunity Grant programs—as well as the information of their parents, spouses, and endorsers.¹⁰ For each individual in those categories, records stored in COD include contact information, SSN, driver’s license number, and financial information.¹¹ COD also contains credit report information for Federal Direct PLUS Loan applicants, recipients, and endorsers.¹²

The most recent SORN for COD was published on June 28, 2023.¹³ It specifies that access to the system is limited to individuals who have undergone a security clearance investigation, and those accessing Privacy Act data “are required to hold, at a minimum, a moderate-risk security clearance level.”¹⁴ ED uses a security system that “limits data access to Department and contract staff on a ‘need-to-know’ basis.”¹⁵ The SORN identifies particular “routine uses” for which ED may disclose records “without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected.”¹⁶

3. Future Act System (FAS)

FAS was created in 2023, and was specifically designed to maintain federal tax information (FTI) that ED receives from the IRS pursuant to sections 6103(l)(13)(A),

¹⁰ *Id.* at 41947.

¹¹ *Id.*

¹² *Id.*

¹³ *Id.* at 41942.

¹⁴ *Id.* at 41951.

¹⁵ *Id.*

¹⁶ *Id.* at 41948–50.

(C), and (D) of the Internal Revenue Code.¹⁷ FAS contains records provided by aid applicants for and aid recipients on the FAFSA, including contact information, date of birth, SSN, and income and asset information, as well as income and asset information of their parents and spouses. The system also contains detailed FTI used to determine eligibility for, and the amount of, Federal student aid, including “adjusted gross income (AGI) amount; total number of tax exemptions; total number of dependents; income earned from work (sum of wages, farm income, Schedule C income); total amount of income tax paid; total allowable education tax credits; sum of untaxed IRA contributions and other payments to qualified plans; tax-exempt interest received; sum of untaxed pensions and annuities; net profit/loss from Schedule C; and indicator of filing for Schedules A, B, D, E, F, and H.”¹⁸ It also contains similar records for applicants to, and participants in, Income-Driven Repayment (IDR) Plans.¹⁹

The SORN for FAS was published on June 29, 2023.²⁰ It specifies that ED’s security system “limits data access to Department and contract staff on a ‘need-to-know’ basis.”²¹ The SORN provides that records contained in FAS may be disclosed without the consent of the individual only for the specific listed routine uses, *and* if

¹⁷ FSA, Notice of a new system of records, Privacy Act of 1974; System of Records, 88 Fed. Reg. 42220, 42220 (June 29, 2023).

¹⁸ *Id.* at 42222.

¹⁹ *Id.*

²⁰ *Id.* at 42220.

²¹ *Id.* at 42225.

such disclosure is consistent with the Internal Revenue Code, 26 U.S.C. § 6103(d)(13).²²

4. Financial Management System (FMS)

“FMS interfaces with other Federal Student Aid systems and consolidates and centralizes all Federal Student Aid accounting and financial data into one system. FMS is a conduit (pass-through system) containing personally identifiable information that is obtained from other Federal Student Aid systems.”²³ It contains, among other things, records for borrowers who are eligible to receive refunds from ED for overpayments or discharges of their Title IV student aid.²⁴ Borrowers may qualify for loan discharges for a wide range of reasons, including that they have a total and permanent disability, that they were victims of forgery on the loan forms, or that the school misled them or violated the law. For these borrowers, FMS “includes a borrowers social security number, name and address, amount of overpayment to be refunded, and name of the loan holder.”²⁵

The SORN for FMS was published on January 2, 2009.²⁶ It specifies that “[t]his system of records limits data access to Department and contract staff on a need-to-

²² *Id.* at 42223.

²³ FSA, Notice of a New System of Records, Privacy Act of 1974; System of Records—Financial Management System (FMS), 73 Fed. Reg. 177, 177 (Jan. 2, 2008).

²⁴ *Id.* at 177, 179.

²⁵ *Id.* at 178.

²⁶ *Id.* at 177.

know basis.”²⁷ The SORN provides that records contained in FMS may be disclosed without the consent of the individual only for the specific listed routine uses, and if the disclosure is compatible with the purposes for which the record was collected.²⁸

DOGE and DOGE’s access to ED’s systems

On the day of his inauguration, President Trump issued an executive order establishing a so-called “Department of Government Efficiency.”²⁹ Under the executive order, the United States Digital Service was renamed the United States DOGE Service (USDS) and a “temporary organization” was established under 5 U.S.C. § 3161 entitled “the U.S. DOGE Service Temporary Organization.”³⁰ The executive order directs the USDS Administrator to “work with Agency Heads to promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization.”³¹ It also directs agency heads to “take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems.”³² The executive order “displaces all prior executive orders and regulations,

²⁷ *Id.* at 179.

²⁸ *Id.* at 178.

²⁹ Executive Order 14158 of January 20, 2025, Establishing and Implementing the President’s “Department of Government Efficiency,” 90 Fed. Reg. 8441 (Jan. 29, 2025).

³⁰ *Id.* at 8441.

³¹ *Id.*

³² *Id.* at 8442.

insofar as they are subject to direct presidential amendment, that might serve as a barrier to providing USDS access to agency records and systems as described above.”³³

Although no formal announcement has been made by the White House, entrepreneur Elon Musk has been widely reported to be the leader of DOGE. Mr. Musk was recently made a special government employee.³⁴ And he has reportedly assembled a team of approximately 40 individuals who “have emerged as his enforcers, sweeping into agency headquarters with black backpacks and ambitious marching orders.”³⁵ Although these individuals plainly work for Mr. Musk, it appears that the individuals are being designated as “employees” of multiple agencies concurrently—perhaps in an attempt to evade privacy and security laws.³⁶ At least sixteen DOGE-affiliated individuals have “landed” at ED, but it is unclear how many of them have been designated as ED “employees.”³⁷ Reporting indicates at least one of these individuals has been concurrently assigned email accounts at ED, the General Services Administration, the Department of Health and Human Services,

³³ *Id.*

³⁴ Nandita Bose & Steve Holland, *Trump makes Musk, the world's richest man, a 'special government employee'*, Reuters (Feb. 3, 2025), <https://www.reuters.com/world/us/trump-makes-musk-worlds-richest-man-special-government-employee-2025-02-03/>; see also 18 U.S.C. § 202(a).

³⁵ Theodore Schleifer, *Young Aides Emerge as Enforcers in Musk's Broadside Against Government*, N.Y. Times (Feb. 7, 2025), <https://www.nytimes.com/2025/02/07/us/politics/musk-doge-aides.html>.

³⁶ *Id.*

³⁷ *Id.*

and the Centers for Disease Control and Prevention; has requested access to Medicare systems; and has also been deployed to the Department of Energy.³⁸ Other DOGE-affiliated individuals that have been given ED email accounts include Jehn Balajadia, Mr. Musk’s assistant, and Edward Cristine, a recent high-school graduate who is reported to have been fired from an internship with a data security company in connection with “the leaking of proprietary company information.”³⁹ At least two members of DOGE have been granted “administrator-level status in the department’s email system.”⁴⁰

Neither ED nor DOGE have said what exactly these people are doing at ED. But reporting indicates that they have been granted wide-ranging access to ED—and the records systems it maintains. On February 3, 2025, the Washington Post reported that individuals affiliated with DOGE had begun working inside ED, and that “[a]t least some” of them had been granted access to “multiple sensitive internal systems, ... including a financial aid dataset that contains the personal information for millions of students enrolled in the federal student aid program.”⁴¹ Mr. Musk responded to this story on his social media platform, X, and connected DOGE’s efforts

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ Tyler Kingkade & Natasha Korecki, *Inside DOGE’s takeover of the Education Department*, NBC News (Feb. 8, 2025), <https://www.nbcnews.com/news/us-news/elon-musk-doge-team-education-department-rcna191244>.

⁴¹ Laura Meckler, et al., *Trump preps order to dismantle Education Dept. as DOGE probes data*, Wash. Post (Feb. 3, 2025), <https://www.washingtonpost.com/education/2025/02/03/trump-education-department-dismantling-executive-order-draft/>.

to the Administration’s goal of “ending the federal Dept of Education.”⁴² Mr. Musk has since expressed the (incorrect) position that there is “no such department in the federal government” as the Department of Education.⁴³ *Cf.* 20 U.S.C. § 3411 (“There is established an executive department to be known as the Department of Education.”).

Additional reporting confirmed that some ED staff members are “deeply alarmed by the fact that DOGE staffers have gained access to federal student loan data, which includes personal information for millions of borrowers,” and noted unnamed “officials” expressing concern “about DOGE’s taking control of government systems that hold Americans’ personal information, including student loan data”—raising privacy and security concerns because of DOGE associates’ failure to comply with protocols.⁴⁴ This concern is consistent with that shared by cyber security experts as to DOGE’s access to other information systems, and government information systems more generally.⁴⁵ On February 5, 2025, the Washington Post reported that DOGE representatives “have fed sensitive data from across the Education Department into artificial intelligence software” of unknown provenance, sparking

⁴² <https://x.com/elonmusk/status/1886633448078475593>.

⁴³ <https://x.com/elonmusk/status/1887971408573018370>.

⁴⁴ Jeff Stein, et al., *U.S government officials privately warn Musk’s blitz appears illegal*, Wash. Post (Feb. 4, 2025), <https://www.washingtonpost.com/business/2025/02/04/elon-musk-government-legal-doge/>.

⁴⁵ See, e.g., Joseph Menn, et al., *Treasury was warned DOGE access to payments marked an ‘insider threat’*, Wash. Post (Feb. 7, 2025), <https://www.washingtonpost.com/national-security/2025/02/07/doge-treasury-payments-system-warning/>.

security concerns.⁴⁶ On February 7, 2025, after this lawsuit was commenced, news organizations reported that DOGE-affiliated individuals have been granted access to COD, NSLDS, FMS, and a fourth system called FSA Partner Connect, which is a portal that higher education institutions use to submit information to ED.⁴⁷ An NBC News article reported concerns within the agency that “Musk and his team would use information from the national student loan database to target Americans.”⁴⁸

In response to this litigation, a spokesperson for ED asserted that “DOGE is supporting [the Education Department] in implementing government-wide civil service reform focused on return to in-person work, restoring accountability for employees who have policy-making authority, restoring accountability for senior career executives, and reforming the federal hiring process to focus on merit.”⁴⁹

⁴⁶ Hannah Natanson, et al., *Elon Musk’s DOGE is feeding sensitive federal data into AI to target cuts*, Wash. Post (Feb. 6, 2025), <https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/>.

⁴⁷ Zachary Schermele, *Students sue Education Department, allege DOGE is accessing private data*, USA Today (Feb. 7, 2025), <https://www.usatoday.com/story/news/education/2025/02/07/students-sue-doge-education-department-musk/78329183007/>; Danielle Douglas-Gabriel, *Consumer groups sue Trump administration over DOGE access*, Wash. Post (Feb. 7, 2025), <https://www.washingtonpost.com/politics/2025/02/07/trump-presidency-news/#link-AFIQUVHY3BF4VHB5UF7HS57W4E>; see also Collin Binkley & Bianca Vázquez Toness, *Musk team’s access to student loan systems raises alarm over borrowers’ personal information*, Associated Press (Feb. 7, 2025), <https://apnews.com/article/education-department-trump-doge-8c5bba3883b3d924b28114a4f291bec4> (reporting that “Musk’s DOGE team already has gained access to a database housing personal information on millions of students and parents with federal student loans, according to two people with knowledge of the issue”).

⁴⁸ Kingkade & Korecki, note 40, *supra*.

⁴⁹ Douglas-Gabriel, note 47, *supra*.

LEGAL STANDARD

To obtain a temporary restraining order, “the moving party must show: (1) a substantial likelihood of success on the merits; (2) that it would suffer irreparable injury if the [temporary restraining order] were not granted; (3) that [such an order] would not substantially injure other interested parties; and (4) that the public interest would be furthered” by the order. *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006) (citations omitted); *see also Hall v. Johnson*, 559 F. Supp. 2d 1, 3 n.2 (D.D.C. 2009) (“[T]he same standard applies to both temporary restraining orders and to preliminary injunctions.” (citation omitted)). “When the movant seeks to enjoin the government, the final two TRO factors—balancing the equities and the public interest—merge.” *D.A.M. v. Barr*, 474 F. Supp. 3d 45, 67 (D.D.C. 2020) (citing *Pursuing Am.’s Greatness v. FEC*, 831 F.3d 500, 511 (D.C. Cir. 2016)).

ARGUMENT

I. Plaintiff has standing.

To be entitled to a temporary restraining order, a plaintiff must demonstrate a “substantial likelihood of standing.” *Nguyen v. U.S. Dep’t of Homeland Sec.*, 460 F. Supp. 3d 27, 33 (D.D.C. 2020) (quoting *Elec. Privacy Inf. Ctr. v. Pres. Advisory Comm’n on Election Integrity*, 878 F.3d 371, 377 (D.C. Cir. 2017)). As demonstrated by the accompanying declarations of Plaintiff’s members Aditi Hariharan, Antonio

Caceres, and Jane Doe, Plaintiff satisfies that requirement here based on its associational standing.⁵⁰

“Associational standing requires that ‘(1) at least one member of the association has standing to sue in her own right (based on a showing of harm, causation, and redressability), (2) the interests the association seeks to protect by suing on its members’ behalf are germane to its purpose, and (3) neither the asserted claim nor the relief requested requires individual members to participate in the litigation.’” *Ctr. for Biological Diversity v. Regan*, 734 F. Supp. 3d 1 (D.D.C. 2024) (quoting *Ctr. for Biological Diversity v. EPA*, 56 F.4th 55, 66 (D.C. Cir. 2022)). These elements are satisfied here.

A. Plaintiff’s members are suffering, and will continue to suffer, harm caused by Defendants’ actions and which is redressable by the relief sought.

⁵⁰ UCSA member Jane Doe submits her declaration pseudonymously given her concerns that publicly identifying as a student in a “mixed-status” family might lead to targeting by the federal government. *See* Doe Decl. ¶ 4. A student is in a “mixed status” family if “[they] are a U.S. citizen or eligible noncitizen, [and their] their parent(s) or spouse (FAFSA contributors) do not have a Social Security number (SSN).” Cal. Student Aid Comm’n, CADAA for Mixed-Status Families, <https://www.csac.ca.gov/cadaa-msf>. An association may rely on evidence of harm to a specific anonymous member to establish standing. *See Advocs. for Highway & Auto Safety v. FMCSA*, 41 F.4th 586, 594 (D.C. Cir. 2022) (“anonymity is no barrier to standing on this record”) (citing *NB ex rel. Peacock v. District of Columbia*, 682 F.3d 77, 86 (D.C. Cir. 2012)); *NAACP v. Trump*, 298 F. Supp. 3d 209, 225 (D.D.C. 2018) (finding associational standing based on anonymous affidavits from organization’s members) (subsequent history omitted); *see also Hotel & Rest. Emps. Union, Loc. 25 v. Smith*, 846 F.2d 1499, 1506 (D.C. Cir. 1988) (“Naming those [union] members adds no essential information bearing on the injury component of standing.”)

UCSA has over 230,000 members, who are the current undergraduate students at the nine campuses of the University of California system. Hariharan Decl. ¶ 3. More than 70% of these student members currently receive federal financial aid via a variety of programs, including Pell Grants, federal work-study, Supplemental Educational Opportunity Grants, and various federal loan programs.⁵¹ To participate in these programs, these students were required by statute to provide ED with detailed personal information, and authorization to access their tax return information. *See* 20 U.S.C. §§ 1090(a)(1), 1098h(a)(1). UCSA members Aditi Hariharan, Antonio Caceres, and Jane Doe provided such information and authorization. Hariharan Decl. ¶ 7; Caceres Decl. ¶ 4; Doe Decl. ¶ 2. These UCSA members’ personal information—like the personal information of tens of thousands of other UCSA members—is stored on ED’s systems, and includes tax return information, SSNs, contact information, marital status, and citizenship status. Defendants’ actions have trampled on Plaintiff’s members’ reasonable expectation that their sensitive personal information will be securely held in accordance with governing law and basic cybersecurity principles, and puts them at an increased risk of interference, fraud, and unauthorized access. *See New York v. Trump*, No. 25 Civ. 1144 (JAV), 2025 WL 435411, at *1 (S.D.N.Y. Feb. 8, 2025) (concluding that DOGE’s access to Treasury systems “presents [a risk] of the disclosure of sensitive and

⁵¹ Univ. of Cal., *The Facts: Federal Financial Aid for UC Students* (Mar. 2021), https://www.ucop.edu/federal-governmental-relations/files/Advocacy/Federal-Research/Fact_Sheet_Federal_Financial_Aid.pdf.

confidential information and the heightened risk that the systems in question will be more vulnerable than before to hacking”).

Allowing DOGE access to Plaintiff’s members’ data caused them immediate and urgent injury. Plaintiff’s members, including Hariharan, Caceres, and Doe, have a constitutionally protected privacy interest in the information they have shared with ED, which they allege has been shared to DOGE affiliates, and will continue to be shared to DOGE affiliates, unlawfully. As the D.C. Circuit has held, “[t]he loss of a constitutionally protected privacy interest itself would qualify as a concrete, particularized, and actual injury in fact. And the ongoing and substantial threat to that privacy interest would be a concrete, particularized, and imminent injury in fact.” *In re OPM Data Sec. Breach Litig.*, 928 F.3d 42, 55 (D.C. Cir. 2019) (per curiam) (emphasis omitted).

While this concrete injury is sufficient to show standing, DOGE’s access to Plaintiff’s members’ personal information has also caused those members emotional distress, which will continue so long as DOGE has access to their information. *See* Hariharan Decl. ¶ 10; Caceres Decl. ¶ 7; Doe Decl. ¶ 7. This emotional harm is also a concrete injury for purposes of standing. *See Ahmed v. Blinken*, No. CV 24-153 (LLA), 2024 WL 4903771, at *3 (D.D.C. Nov. 27, 2024) (finding emotional harm sufficient to satisfy Article III injury-in-fact requirement in Administrative Procedure Act case); *Thompson v. Trump*, 590 F. Supp. 3d 46, 71 (D.D.C. 2022), *aff’d on other grounds sub nom. Blassingame v. Trump*, 87 F.4th 1 (D.C. Cir. 2023) (finding “emotional harm sufficiently concrete to establish Article III standing”, and discussing common law

history); *Magruder v. Cap. One, N.A.*, 540 F. Supp. 3d 1, 8 (D.D.C. 2021) (recognizing that a plaintiff can “establish an Article III injury based on emotional harm if that alleged harm stems from the infringement of some legally protected ... or judicially cognizable interest that is either recognized at common law or specifically recognized as such by the Congress” (quoting *Al-Aulaqi v. Obama*, 727 F. Supp. 2d 1, 25 (D.D.C. 2010)); cf. *Hancock v. Urb. Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (acknowledging emotional injury caused by privacy violation may be sufficient to demonstrate standing).

The risks that flow from Defendants’ disclosures create additional cognizable injuries. Given the nature of the personal information shared with DOGE, DOGE’s reported uploading of data to artificial intelligence systems hosted on non-government servers, DOGE’s failures to comply with security protocols, and the fact that one DOGE-affiliated individual who reportedly has access to ED systems was associated with a data breach in the past, discussed above at p. 13, *supra*, “it is at least plausible that [plaintiff’s members] run a substantial risk” of identity theft. *In re OPM Data Breach*, 928 F.3d at 58.

The fact that many DOGE-affiliated individuals are concurrently working at several federal agencies also suggests a substantial risk that Plaintiff’s members’ data will be shared with other agencies and/or used for unauthorized purposes, including immigration enforcement. Individuals within ED have expressed concerns that this will occur.⁵² The risk has already had a concrete chilling effect, discouraging

⁵² See, e.g., Kingkade & Korecki, note 40 *supra*.

students and their families from applying for aid—or attending college at all. *See* Hariharan Decl. ¶ 11; Doe Decl. ¶ 8; Caceres Decl. ¶ 8. One nonprofit has already begun discouraging students whose family members may be undocumented from applying for federal student aid as a result of DOGE’s access to ED’s systems, and fears as to how this data may be disseminated.⁵³ Plaintiff’s members include a substantial number of students from mixed-status families, including UCAS member Doe. *See* Hariharan Decl. ¶ 6; Doe Decl. ¶ 4. The California Student Aid Commission has estimated that up to 12,000 students from mixed-status families may be enrolled at the University of California.⁵⁴

These harms are the direct result of Defendants’ actions and could be redressed by an order of this Court prohibiting continued access to ED’s systems, and restricting the use of records already unlawfully obtained—thus satisfying the causation and redressability requirements.

B. The other requirements of associational standing are satisfied.

UCSA easily satisfies the other two requirements of associational standing. This action is germane to the organization’s mission: protecting the interests of University of California students. *See* Hariharan Decl. ¶¶ 3–4. And individual member participation is not necessary in this case given the nature of Plaintiff’s

⁵³ *See* Liam Knox & Jessica Blake, *Is DOGE Digging Around in Student Data?*, Inside Higher Ed (Feb. 8, 2025), <https://www.insidehighered.com/news/government/politics-elections/2025/02/08/doges-access-education-department-data-raises>.

⁵⁴ Univ. of Cal., Office of the President, Memo to Members of the Acad. & Student Affs. Cmte. of the Regents of the Univ. of Cal., *Financial Aid Experience for Students*, Jan. 2025, <https://regents.universityofcalifornia.edu/regmeet/jan25/a4.pdf>.

Administrative Procedure Act (APA) claims and because “Plaintiff[] seek[s] prospective and injunctive relief, not damages for its members.” *Powder River Basin Res. Council v. U.S. Dep’t of Interior*, No. 22-CV-2696 (TSC), 2024 WL 4188655, at *5 (D.D.C. Sept. 13, 2024); *see also NRDC v. Raimondo*, No. CV 23-982 (BAH), 2024 WL 4056653, at *15 (D.D.C. Sept. 5, 2024).

II. Plaintiff is likely to succeed on the merits.

Defendants’ action to grant DOGE-affiliated individuals access to ED’s systems is a final action that may be challenged under the APA. *Venetian Casino Resort, LLC v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008) (holding agency’s “policy of permitting employees to disclose information without notice” was reviewable final agency action under the APA). Plaintiff is likely to prevail on its claims that this act should be held unlawful and set aside as contrary to law, in excess of statutory authority, and arbitrary and capricious. *See* 5 U.S.C. § 706(2).

A. Defendants’ action giving DOGE access to ED’s records is contrary to law and in excess of their statutory authority.

“Agencies must operate within the legal authority conferred by Congress,” and “courts have the responsibility to determine whether ‘individual rights’ have been infringed ‘by the exertion of unauthorized administrative power.’” *Med. Imaging & Tech. All. v. Libr. of Cong.*, 103 F.4th 830, 838 (D.C. Cir. 2024) (quoting *Stark v. Wickard*, 321 U.S. 288, 309–10 (1944)). Under the APA, when an agency’s action is “not in accordance with law,” courts have a duty to set it aside. 5 U.S.C. § 706(2)(A). Even apart from the APA, courts may enjoin *ultra vires* actions by an agency that are in excess of its statutory authority. *Ctr. for Biological Diversity v. Trump*, 453 F.

Supp. 3d 11, 50 (D.D.C. 2020). An agency's decision to disclose information in violation of law is the type of agency action for which the courts can provide redress. *Chrysler Corp. v. Brown*, 441 U.S. 281, 318–19 (1979) (discussing reverse-FOIA actions).

Here, any statutory authority Defendants would otherwise have to authorize individuals associated with DOGE to access the sensitive personal and financial information stored in ED's records is constrained by the Privacy Act and section 6103 of the Internal Revenue Code. There is no question that the records at issue here are records about individuals covered by the Privacy Act: "information about an individual that is maintained by an agency" and that identifies the individual. 5 U.S.C. § 552a(a)(4). Indeed, ED published SORNs in the Federal Register precisely because it recognized that the personal information it obtains about students and their families is protected by the Privacy Act.

The Privacy Act prohibits Defendants from disclosing ED's records on individuals to any person or any agency without the consent of the individual affected, unless an express exception applies. Defendants did not obtain individual consent before allowing DOGE-affiliated individuals to access ED's records, and none of the statutory exceptions applies to DOGE's activities. For instance, one exception allows disclosure to "officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." *Id.* § 552a(b)(1). But DOGE-affiliated individuals are neither "officers and employees" of ED, nor do they have a need for Plaintiff's members' records in the performance of their duties.

To start, the reported facts of DOGE-affiliated individuals' concurrent "employment" at multiple agencies suggest that such a designation would be an illegitimate attempted end-run around privacy law. In addition, while some DOGE-affiliated individuals may claim to have been detailed to ED and thus qualify as "employees," such detailing is not permitted by the relevant statute. DOGE was created as a "temporary organization" within the Executive Office of the President, pursuant to 5 U.S.C. § 3161. While section 3161 provides for employees of a "department or agency" to be detailed *to* a temporary organization, it does not provide any authority for a detail of employees of temporary organizations to agencies like ED. Nor does 31 U.S.C. § 1535(a), which authorizes details from one agency to another. President Trump's executive order creating DOGE made clear that he did not intend for DOGE to be an "agency," as he defined that term to exclude DOGE and other components of the Executive Office of the President, and repeatedly distinguished between DOGE and "agencies." *See* 90 Fed. Reg. at 8441. And DOGE is not an agency under the Administrative Procedure Act, as it does not wield "substantial independent authority." *Elec. Priv. Info. Ctr. v. Nat'l Sec. Comm'n on A.I.*, 466 F. Supp. 3d 100, 109 (D.D.C. 2020) (reviewing case law and concluding temporary organization was not an "agency"). To the contrary, DOGE is solely dedicated "to advancing the President's 18-month DOGE agenda." 90 Fed. Reg. at 8442. If an entity's "sole function is to advise and assist the President," it is not an agency. *Armstrong v. Exec. Office of the Pres.*, 90 F.3d 553, 558 (D.C. Cir. 1996).

Moreover, even assuming (counter-factually) that these individuals qualify as ED “employees” as used in the statute, they still do not fall within the scope of 5 U.S.C. § 552a(b)(1) because they do not have any “need” to access students’ protected information—as the President has conceded. *See* Transcript, note 1, *supra*. Whatever the lawfulness of DOGE’s work on “civil service reform” or its goal of shutting down a congressionally created agency, they do not demonstrate a need to access the personal and financial information of students like Plaintiffs’ members.

Similarly, the routine-use exception does not apply. None of ED’s lists of routine uses in the SORNs discussed above suggest that records could be accessed and used by DOGE-affiliated individuals as a tool for the administration to use in its goals of eliminating the Department of Education, or “civil service reform.” And the SORNs for FAS, FMS, and COD each explicitly specify that access will only be granted on a “need to know” basis.⁵⁵ No such need exists here. Further, there is no evidence that DOGE officials have received the security clearances and trainings required by the SORNs at issue here. And in any event, “agencies covered by the Privacy Act may not utilize the ‘routine use’ exception to circumvent the mandates of the Privacy Act.” *Doe v. Stephens*, 851 F.2d 1457, 1466 (D.C. Cir. 1988).

With respect to tax records protected by 26 U.S.C. § 6103 and 20 U.S.C. § 1098h, the prohibition on sharing of information is even more straightforward. Section 6103(l)(13) permits only those at ED who meet the statutory definition of

⁵⁵ 88 Fed. Reg. at 42220 (FAS); 88 Fed. Reg. at 41951 (COD); 73 Fed. Reg. at 179 (FMS).

“authorized persons” to access tax return information, and only for specific purposes. DOGE-affiliated individuals who are not ED employees cannot be “authorized persons” under 26 U.S.C § 6103. And neither abolishing the Department of Education nor “[g]overnment-wide civil service reform” is one of the purposes for which ED employees may be granted access. To the extent that ED has authorized disclosure of tax information for these purposes, or for any purpose other than those contained in section 6103(l)(13), or to individuals who do not meet the statutory definition of “authorized person,” its action is unlawful under section 6103.

B. Defendants’ action is arbitrary and capricious.

Plaintiff is also likely to succeed on its claim that Defendants’ decision to permit DOGE-affiliated individuals to access restricted information is arbitrary and capricious. The APA “requires agencies to engage in ‘reasoned decisionmaking.’” *Dep’t of Homeland Sec. v. Regents of the Univ. of California*, 591 U.S. 1, 16 (2020) (quoting *Michigan v. EPA*, 576 U.S. 743, 750 (2015)). An agency’s decision is arbitrary if the agency “failed to consider an important aspect of the problem.” *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

Here, Defendants have reversed ED’s longstanding policy fully protecting individuals’ personal information, and of denying access to individuals who have no need for that information. *See, e.g.*, 34 C.F.R. § 5b.3 (recognizing ED’s policy “to protect the privacy of individuals to the fullest extent possible”); *id.* § 5b.9(b) (limiting disclosures without consent). In doing so, Defendants failed to engage in reasoned decisionmaking. Not only did Defendants fail to take account of their legal obligations under federal law to protect personal information contained in their records, they

ignored the reliance and expectation interests that current and former students, their spouses, and parents have with respect to the privacy of the personal information they must share with ED to participate in programs created by Congress. Even putting aside that Defendants lack authority to invite DOGE into ED's systems to view people's personal data for their own purposes, giving access to this sensitive information to the nebulous DOGE entity lacks a rational basis and is unreasonable—particularly in light of the President's concession that DOGE has no need to access that information. *See* Transcript, note 1, *supra*.

III. Plaintiff will suffer immediate, irreparable injury if Defendants continue to allow unlawful access to ED's records on individuals.

Plaintiff's members are suffering, and will continue to suffer, irreparable injury from Defendants' ongoing exposure of their sensitive personal and financial data to third-party access. "An irreparable harm is an imminent injury that is both great and certain to occur, and for which legal remedies are inadequate." *Beattie v. Barnhart*, 663 F. Supp. 2d 5, 9 (D.D.C. 2009). Defendants have allowed third parties unlawful access to Plaintiff's members' private information and, unless enjoined, will continue to grant such access. The injury, then, is not only imminent and certain—it is already occurring. Equitable relief is needed to end Defendants' ongoing exposure of highly vulnerable information, such as the Social Security numbers, bank account details, and home addresses and telephone numbers of Plaintiff's members. Every additional moment that this information remains accessible to unauthorized third parties compounds the injury to individual privacy by increasing the opportunity for further dissemination. *See New York v. Trump*, 2024 WL 435411, at *1 (granting

temporary restraining order based on “risk of the disclosure of sensitive and confidential information and the heightened risk that the systems in question will be more vulnerable than before to hacking” posed by DOGE’s access to Treasury data).

As discussed above, *see pp. 20–24, supra*, this access has injured Plaintiff’s members’ privacy interests, caused emotional harm, had a chilling effect, created a risk of further unlawful disclosure, and placed them at a risk of identity theft. Hariharan Decl. ¶¶ 8–12; Caceres Decl. ¶¶ 5–9; Doe Decl. ¶¶ 5–9. The protections enshrined in the Privacy Act and the Internal Revenue Code reflect Congress’s sound judgment that individuals have a right to expect that access to the sensitive information that they share with the government will be strictly limited. 5 U.S.C. § 552a(e)(10) (requiring agencies to “insure the security and confidentiality” of federal records subject to the Privacy Act to protect against “substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom” the records are maintained); *see Cause of Action v. IRS*, 125 F. Supp. 3d 145, 163 (D.D.C. 2015) (noting that the “core purpose” of section 6103” of the Internal Revenue Code “is to ‘protect[] taxpayer privacy.’” (alteration in original; quoting *Church of Scientology of Cal. v. IRS*, 484 U.S. 9, 16 (1987))). By allowing third parties access to confidential information that Congress sought to protect, Defendants have established a total and ongoing injury to the privacy rights of Plaintiff’s members. *Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 76 (D.D.C. 2009) (observing that if “proprietary, privileged, and confidential information” were “used and/or continue[d]

to be disclosed” during the pendency of a lawsuit challenging such use and disclosure, “the very rights [the lawsuit] seeks to protect will have been destroyed”).

This ongoing injury cannot be remedied after the fact. “Obviously, once ... highly personal information is disclosed ..., the revelation cannot be undone.” *Nat’l Treasury Emps. Union v. U.S. Dep’t of Treasury*, 838 F. Supp. 631, 640 (D.D.C. 1993); *see also Hospitality Staffing Sols., LLC v. Reyes*, 736 F. Supp. 2d 192, 200 (D.D.C. 2010) (“This Court has recognized that the disclosure of confidential information can constitute an irreparable harm because such information, once disclosed, loses its confidential nature.”); *Wilcox v. Bastiste*, No. 2:17-cv-122, 2017 WL 2525309, at *3 (E.D. Wash. 2017) (“In the age of the internet, when information is made public quickly and without borders, it is nearly impossible to contain an impermissible disclosure after the fact[.]”). And the longer that the private information of Plaintiff’s members remains accessible to unauthorized third parties, the greater the irreparable injury is. After all, as long as the sensitive data of Plaintiff’s members remains accessible to DOGE-affiliated individuals, the more opportunity there is for that data to be disclosed to still more unauthorized third parties, either accidentally or deliberately.

What is more, many of Plaintiff’s members who are presently experiencing progressively worsening injury to their privacy rights would not even be eligible for retrospective monetary damages if they were required to seek relief in that form. Under *FAA v. Cooper*, 566 U.S. 284 (2012), damages for a Privacy Act violation are available only to those individuals who can establish “proven pecuniary or economic

harm,” *id.* at 299, because Congress declined to waive sovereign immunity for claims of “nonpecuniary harm, even if such harm can be proved,” *id.* at 301. For those individuals whose privacy rights have been—and continue to be—violated by Defendants but who have not experienced resultant economic losses, damages are not even arguably a means of ameliorating the irreparable injuries that Defendants are presently inflicting.

Ultimately, absent a temporary restraining order from this Court, Plaintiff’s members will continue to experience invasions their privacy that are incapable of being undone.

IV. The balance of equities and the public interest support grant of a TRO.

As against the certain and irreparable injury that innumerable members of the public—including Plaintiff’s members—are presently experiencing as a result of Defendants’ unlawful actions, Defendants would suffer no cognizable harm if enjoined from continuing to perpetrate those actions. After all, “[i]t is well established that the Government ‘cannot suffer harm from an injunction that merely ends an unlawful practice.’” *C.G.B. v. Wolf*, 464 F. Supp. 3d 174, 218 (D.D.C. 2020) (quoting *Open Cmities. Alliance v. Carson*, 286 F. Supp. 3d 148, 179 (D.D.C. 2017)). Moreover, Defendants would suffer no injury from remaining bound by the same confidentiality restrictions that bound them as recently as last month, before DOGE came into existence—and certainly no reason why Defendants would suffer injury from being temporarily barred from granting DOGE access to confidential materials during the period in which this Court assesses whether such access is lawful. This is particularly

clear given the President’s concession that DOGE does not need access to Americans’ personal information. *See* Transcript, note 1, *supra*. The balance of equities thus tips decisively in favor of granting temporary relief here.

Meanwhile, a temporary restraining order would serve the public interest. “There is generally no public interest in the perpetuation of an unlawful agency action.” *Open Cmities. Alliance*, 286 F. Supp. 3d at 179 (citation omitted). “To the contrary, there is a substantial public interest in having governmental agencies abide by the federal laws.” *Id.* (citation omitted).

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that this Court grant its motion and enter a temporary restraining order enjoining Defendants from disclosing information about individuals to individuals affiliated with DOGE, and enjoining Defendants to retrieve and safeguard any such information that has already been obtained by and shared or transferred by DOGE or individuals associated with it.

Dated: February 10, 2025

Respectfully submitted,

/s/ Adam R. Pulver

Adam R. Pulver (DC Bar #1020475)

Nandan M. Joshi (DC Bar # 456750)

Public Citizen Litigation Group

1600 20th Street NW

Washington, DC 20009

(202) 588-1000

apulver@citizen.org

Daniel A. Zibel (DC Bar No. 491377)

Alexander S. Elson (DC Bar No. 1602459)

Tyler S. Ritchie

(DC Bar No. 90018119)
National Student Legal Defense Network
1701 Rhode Island Ave. NW
Washington, DC 20036
(202) 734-7495