No. 24A_____

In the Supreme Court of the United States

SOCIAL SECURITY ADMINISTRATION, ET AL., APPLICANTS

v.

AMERICAN FEDERATION OF STATE, COUNTY AND MUNICIPAL EMPLOYEES, AFL-CIO, ET AL.

APPLICATION FOR A STAY OF THE INJUNCTION ISSUED BY THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND AND REQUEST FOR AN ADMINISTRATIVE STAY

D. JOHN SAUER
Solicitor General
Counsel of Record
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

TABLE OF CONTENTS

PARTIES TO THE PROCEEDING

Applicants (defendants-appellants below) are the Social Security Administration; Leland Dudek, Acting Commissioner of the Social Security Administration; Scott Coulter, Chief Information Officer, Social Security Administration*; Elon Musk, Senior Advisor to the President; U.S. DOGE Service; U.S. DOGE Service Temporary Organization; and Amy Gleeson, DOGE Acting Administrator.

Respondents (plaintiffs-appellees below) are the American Federation of State, County and Municipal Employees, AFL-CIO; the American Federation of Teachers; and the Alliance for Retired Americans.

RELATED PROCEEDINGS

United States District Court (D. Md.):

American Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. *SSA*, No. 25-CV-596 (Mar. 20, 2025) (TRO)

American Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA, No. 25-CV-596 (Apr. 17, 2025) (preliminary injunction)

American Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA, No. 25-CV-596 (Apr. 22, 2025) (motion to stay preliminary injunction)

United States Court of Appeals (4th Cir.):

American Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA, No. 25-1411 (Apr. 30, 2025) (stay of preliminary injunction pending appeal)

American Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA, No. 25-1411 (Apr. 1, 2025) (stay of TRO pending appeal)

---

* Mr. Coulter was automatically substituted for former Chief Information Officer Mike Russo.

In the Supreme Court of the United States

No. 24A_____

SOCIAL SECURITY ADMINISTRATION, ET AL., APPLICANTS

v.

AMERICAN FEDERATION OF STATE, COUNTY AND MUNICIPAL EMPLOYEES, AFL-CIO, ET AL.

APPLICATION FOR A STAY OF THE INJUNCTION ISSUED BY THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND AND REQUEST FOR AN ADMINISTRATIVE STAY

Pursuant to Rule 23 of the Rules of this Court and the All Writs Act, 28 U.S.C. 1651, the Solicitor General—on behalf of applicants the Social Security Administration (SSA), et al.—respectfully files this application for a stay of the preliminary injunction issued by the United States District Court for the District of Maryland (App., *infra*, 169a-174a), pending the consideration and disposition of the government's appeal to the United States Court of Appeals for the Fourth Circuit and, if the court of appeals affirms the injunction, pending the timely filing and disposition of a petition for a writ of certiorari and any further proceedings in this Court. In addition, the Solicitor General respectfully requests an immediate administrative stay of the district court's order pending the Court's consideration of this application.

This emergency application presents a now-familiar theme: a district court has issued sweeping injunctive relief without legal authority to do so, in ways that inflict ongoing, irreparable harm on urgent federal priorities and stymie the Executive Branch's functions. Here, the President adopted an "18-month" Department of

Government Efficiency (DOGE) agenda "to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." Exec. Order No. 14,158, §§ 3(b), 4(a), 90 Fed. Reg. 8441, 8441 (Jan. 20, 2025). The U.S. DOGE Service (USDS) advises the Executive Branch and federal agencies as to how to streamline government, eliminate waste, ferret out fraud, and modernize outdated systems that let malfeasance and inefficiency go undetected. To that end, multiple agencies, including the SSA, the Departments of Treasury and Education, and the Office of Personnel Management (OPM), have created DOGE-supported teams of agency personnel to support this critical government effort for their agencies. These teams have a business need to access the data at their assigned agency and subject the government's records to much-needed scrutiny.

In response, the district court issued a preliminary injunction that compels the SSA to block access to the agency's record systems for DOGE team members and "DOGE Affiliate[s]" unless a host of judicially imposed conditions are met. App., *infra*, 169a-174a. That action followed another district court's decision to block access at Education, Treasury, and OPM. The Fourth Circuit subsequently stayed the three-agency order, see *American Fed'n of Teachers (AFT)* v. *Bessent*, 2025 WL 1023638 (Apr. 7, 2025), and the Fourth Circuit denied "initial hearing en banc," *id.* at *1—yet the Fourth Circuit inexplicably reversed course here.

As a result, the district court is forcing the Executive Branch to stop employees charged with modernizing government information systems from accessing the data in those systems because, in the court's judgment, those employees do not "need" such access. The injunction involving the SSA does not merely halt the Executive Branch's critically important efforts to improve its information-technology infrastructure and eliminate waste. District court control of decisions about internal access to infor-

mation also constitutes inappropriate superintendence of a coequal branch. And the preliminary injunction comes after a temporary restraining order (TRO); collectively, the district court's orders have already stopped the Executive Branch from carrying out key policy objectives in an important federal agency for more than a month. The government cannot eliminate waste and fraud if district courts bar the very agency personnel with expertise and the designated mission of curtailing such waste and fraud from performing their jobs.

This case justifies this Court's intervention, because the district court made glaring legal errors in the course of halting high-priority functions within a key agency. To start, respondents—two labor unions and an advocacy organization whose members have submitted their personal information to the government—lack Article III standing on two independent grounds. Respondents' members furnished their information with the understanding that government employees could access it for a number of purposes, as those employees are permitted to do pursuant to various exceptions in the Privacy Act of 1974 (Privacy Act), 5 U.S.C. 552a. Respondents cannot plausibly claim any concrete injury from having *particular* agency employees—*i.e.*, members of the SSA DOGE team—access their information when those employees are subject to the same legal and ethical obligations against further dissemination that bind all agency employees. Respondents do not suffer any concrete injury based on *which* SSA employees have access to their data subject to those safeguards.

Further, the district court based its injunction on the Administrative Procedure Act (APA), 5 U.S.C. 551 *et seq.*, 701 *et seq.*, yet the basic requirement of an APA suit is missing: there is no "final agency action" to review, such as a binding agency rule or policy. 5 U.S.C. 704. As this Court has recognized, that requirement prevents courts from reviewing "day-to-day operations" of federal agencies under the guise of

APA review. *Lujan* v. *National Wildlife Fed'n*, 497 U.S. 871, 899 (1990). Yet here, the district court is installing itself as the supervisor of the SSA's routine operational decisions such as whether to grant certain employees access to certain systems of records. Left undisturbed, this preliminary injunction will only invite further judicial incursions into internal agency decision-making.

In addition, the order bases that interference on an unsupportable application of the Privacy Act, which authorizes employees to access records when the employees "need" such access. 5 U.S.C. 552a(b)(1). That standard is clearly met here; employees charged with modernizing government information systems and routing out fraud, waste, and abuse in data systems plainly need access to those systems. Yet the district court instead viewed agency employees within the SSA DOGE team as the equivalent of intruders who break into hotel rooms. District courts should not be able to wield the Privacy Act to substitute their own view of the government's "needs" for that of the President and agency heads.

The pendency of this injunction imposes ever-mounting irreparable harm as the district court continues to commandeer basic functions of the Executive Branch. The injunction expresses the district court's view that the Executive Branch cannot correct well-documented problems with its technological systems and combat fraud, waste, and abuse in federal programs using the personnel the Executive Branch has deemed most suited for the task. As noted above, another judge within the District of Maryland previously adopted the same reasoning in issuing a preliminary injunction against three other agencies, but the Fourth Circuit stayed that materially similar order. And myriad other suits seeking to second-guess how agencies share data are close on their heels, threatening to further upend the government's modernization

efforts.[1]

While the injury to the government is immediate and consequential, respondents suffer no irreparable harm based on which employees at an agency may access their data—as a panel of the Fourth Circuit recognized in a materially similar case, see *Bessent*, 2025 WL 1023638, at *6-*7 (Richardson, J., concurring), and three other district courts have recognized about the plaintiffs in materially similar lawsuits, see *University of Cal. Student Ass'n* v. *Carter*, No. 25-cv-354, 2025 WL 542586, at *5 (D.D.C. Feb. 17, 2025); *Electronic Privacy Info. Ctr.* v. *U.S. Office of Pers. Mgmt.*, No. 25-cv-255, 2025 WL 580596, at *6-*7 (E.D. Va. Feb. 21, 2025); *Alliance for Retired Ams.* v. *Bessent*, No. 25-cv-313, 2025 WL 740401, at *20-*24 (D.D.C. Mar. 7, 2025). The balance of equities therefore strongly weighs in the government's favor. This Court should step in.

STATEMENT

1. On January 20, 2025, the President signed Executive Order 14,158, aimed at "modernizing Federal technology and software to maximize governmental efficiency and productivity." § 1, 90 Fed. Reg. 8441 (USDS EO). The USDS EO renamed the preexisting United States Digital Service as the United States DOGE Service (USDS), moved it out of the Office of Management and Budget, and established it as a standalone component within the Executive Office of the President. The EO further established within USDS a temporary organization known as "the U.S. DOGE

---

[1] See, *e.g.*, *Alliance for Retired Ams.* v. *Bessent*, No. 25-313 (D.D.C. filed Feb. 3, 2025); *AFL-CIO* v. *Department of Labor*, No. 25-cv-339 (D.D.C. filed Feb. 5, 2025); *New York* v. *Trump*, No. 25-cv-1144 (S.D.N.Y. filed Feb. 7, 2025); *National Treasury Emps. Union* v. *Vought*, No. 25-cv-380 (D.D.C. filed Feb. 9, 2025); *AFL/CIO* v. *OPM*, No. 25-cv-1237 (S.D.N.Y. filed Feb. 10, 2025); *EPIC* v. *OPM*, No. 25-255 (E.D.Va. filed Feb. 11, 2025); *Nemeth-Greenleaf* v. *OPM*, No. 25-cv-407 (D.D.C. filed Feb. 11, 2025); *Gribbon* v. *Musk*, No. 25-cv-422 (D.D.C. filed Feb. 12, 2025); *Center for Taxpayer Rights* v. *IRS*, No. 25-cv-457 (D.D.C. filed Feb. 17, 2025).

Service Temporary Organization." *Id.* § 3(b); see *id.* § 3(a).

The EO requires each "[a]gency [h]ead"—*i.e.*, the highest-ranking official in each agency—to establish within each agency a "DOGE Team" consisting of agency employees (which may include special government employees). USDS EO §§2(b), 3(c). The EO further charges the USDS Administrator with "commenc[ing] a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." *Id.* § 4(a). And the EO directs the USDS Administrator to collaborate with agency heads to modernize the federal government's technology and software infrastructure to "promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization." *Ibid.*

Critically, to accomplish those objectives, the EO directs the USDS Administrator and agency heads to work together to ensure that USDS has access to "unclassified agency records, software systems, and IT systems" to the "extent consistent with law." USDS EO § 4(b). The EO further provides that "USDS shall adhere to rigorous data protection standards." *Ibid.*

The EO addresses the government's well-documented, urgent need to update and improve its information technology systems to promote efficiency and identify fraud. The Government Accountability Office (GAO) has found that "[i]mproper payments and fraud are long-standing and significant problems in the federal government," with "cumulative improper payment estimates by executive branch agencies" totaling about $2.7 trillion since fiscal year 2003. GAO, GAO-24-107660, *Payment Integrity: Significant Improvements Are Needed to Address Improper Payments and Fraud* 1 (Sept. 10, 2024), https://www.gao.gov/assets/gao-24-107660.pdf. Most relevant here, the GAO has identified SSA's Supplemental Security Income program as

one of six program areas that together "were responsible for approximately $200 billion of the $236 billion fiscal year 2023 improper payments estimate." *Ibid.* GAO therefore found it "critical that actions are taken to enhance payment integrity and reduce improper payments in these programs." *Id.* at 10.

2. a. Applicants are the SSA, the USDS, the U.S. DOGE Service Temporary Organization, and several agency officials in their official capacities. SSA maintains systems of records that contain personally identifiable information of individuals. App., *infra*, 35a-37a. Consistent with the USDS EO, SSA established a DOGE Team of SSA employees and authorized a limited number of team members to access certain information technology systems to carry out the EO. *Id.* at 24a & n.1.

b. Respondents are "two national labor and membership associations and one grassroots advocacy organization." App., *infra*, 25a. They filed this lawsuit on February 21, 2025, and filed an amended complaint on March 7, 2025. Respondents' amended complaint includes seven causes of action. Most relevant here, four counts (Counts 1, 3-5) allege violations of the APA, 5 U.S.C. 706(2), and one count (Count 2) alleges a violation of the Privacy Act, Pub. L. No. 93-579, 88 Stat. 1896. The remaining counts allege *ultra vires* actions by the DOGE defendants (Count 6) and violation of the Appointments Clause, Const. Art. II, § 2, Cl. 2 (Count 7). See App., *infra*, 28a-29a.

c. As noted above, this lawsuit was not the first of its kind. Most relevant here, on February 10, 2025, individual and organizational plaintiffs filed a materially similar lawsuit in the District of Maryland; their complaint focused on access to records systems at the Departments of Treasury and Education and OPM. On February 24, 2025—three days after the original complaint here was filed—a different district court in the District of Maryland entered a TRO against Education, OPM, and their

then-Acting agency heads. See *AFT* v. *Bessent*, 25-cv-430 D. Ct. Doc. 38 (D. Md. Feb. 24, 2025) (*Bessent* TRO Op.). That TRO enjoined the defendants from "disclosing the personally identifiable information of the [individual] plaintiffs and the members of the plaintiff organizations to any DOGE affiliates" or agency employees "working principally on the DOGE agenda," with a single exception at OPM. *Id.* at 32-33.[2]

d. On March 20, 2025, the district court here granted plaintiffs a TRO enjoining the SSA and related defendants (the applicants here) from permitting DOGE team members to access certain SSA records. Specifically, the TRO compelled the applicants not to grant access to any SSA system of records to "DOGE," USDS, "members of the DOGE Team established at" the SSA, certain named individuals, and "any DOGE Affiliate," defined to include any SSA employee working "directly or indirectly" with the DOGE team, unless a host of judicially imposed conditions were met. D. Ct. Doc. 48, at 1-2 (Mar. 20, 2025). The court's 134-page TRO decision relied heavily on the *Bessent* district court's analysis with respect to each of the TRO's key legal rulings. See D. Ct. Doc. 49 (Mar. 20, 2025), at 80-81 (standing); *id.* at 116, 121 (the Privacy Act's "need" exception); *id.* at 127, 129 (irreparable harm).

The following day, the district judge here issued two *sua sponte* "letter[s] to counsel" to clarify the scope of the TRO in response to "several news reports" regarding the agency's purported understanding of the order. D. Ct. Docs. 51-52 (Mar. 21, 2025). In the first letter, the court disputed "assertions" in "news reports" about Acting Commissioner Dudek's purported "belie[f]s" regarding the scope of the TRO. D. Ct. Doc. 51, at 1. In the second letter—issued the same day—the court again

---

[2] The *Bessent* district court declined to enter relief against the Department of the Treasury or Secretary Bessent at that time, because another district court had entered a preliminary injunction that "include[d] Treasury records with the plaintiffs' [personally identifiable information]." *Bessent* TRO Op. 2 n.1.

faulted the Acting Commissioner for news reports regarding the scope of the TRO and stated that the government should have "contact[ed] Chambers *immediately* if there [was] any need for clarification of the TRO." D. Ct. Doc. 52, at 2.

Applicants appealed and sought a stay pending appeal of the district court's TRO in this case pending appeal. The court of appeals dismissed the appeal for lack of jurisdiction, presumably on the theory that TROs are unappealable. C.A. Doc. 18 (Apr. 1, 2025) (stating only that "the appeal is dismissed for lack of jurisdiction"); but see *Department of Educ.* v. *California*, 145 S. Ct. 966, 968 (2025) (per curiam).

3. The *Bessent* case continued to proceed ahead of this one.

a. On March 24, 2025—after expedited briefing and a hearing—the *Bessent* district court issued a preliminary injunction against Education, Treasury, and OPM. *AFT* v. *Bessent*, No. 25-430, 2025 WL 895326 (D. Md.). That preliminary injunction enjoined the agencies from "disclosing the personally identifiable information of the plaintiffs and members of the plaintiff organizations to any DOGE affiliates, defined as individuals whose principal role is to implement the DOGE agenda as described in Executive Order 14,158 and who were granted access to agency systems of records for the principal purpose of implementing that agenda." *Id.* at *32-*33.

As grounds for that injunction, the district court determined that the plaintiffs had Article III standing to challenge the agencies' disclosure of records in government databases to government employees. The court analogized respondents' alleged injury—that "DOGE affiliates have invaded their privacy by obtaining their personal information"—to "the common law tort of intrusion upon seclusion." *Bessent*, 2025 WL 895326, at *10. The court stated that although the plaintiffs "gave their private information to the government" knowing that some government employees would ac-

cess it, they did so "with the expectation that the government would not disclose it to anyone within the government who was not authorized to access it." *Ibid.* The district court also held that the plaintiffs in *Bessent* adequately identified "final agency action" for purposes of the APA. 5 U.S.C. 704. The court characterized each agency's decision to provide access to a handful of government employees as agency "policy" decisions that were "final," because "[t]he decisions to grant access were neither tentative nor interlocutory in nature." *Bessent*, 2025 WL 895326, at *14-*15.

Turning to the merits, the *Bessent* district court determined that the plaintiffs were likely to succeed on their claim that granting access to agency DOGE team members violated the Privacy Act. The court recognized that the Privacy Act allows agency employees to access agency records when they "have a need for the record in the performance of their duties." 5 U.S.C. 552a(b)(1); see *Bessent*, 2025 WL 895326, at *18. But the court held that the government had not adequately established the DOGE employees' need for access. *Id.* at *18-*28. As to the remaining preliminary-injunction factors, the court found that the plaintiffs were "likely to suffer actual and imminent harm" from continued agency access to their private information, "without injunctive relief." *Id.* at *29. The court stated that the threatened "ongoing violation of the plaintiffs' privacy interests" was irreparable because "[a] final judgment of money damages or a permanent injunction would not make them whole." *Id.* at *31. Finally, the court held that because it had found the agencies' actions likely unlawful, "[p]reventing the government's unauthorized disclosure of the plaintiffs' sensitive personal information is in the public interest," and that the preliminary injunction would not cause cognizable injury to the government. *Ibid.*

b. On April 7, 2025, the court of appeals granted the government's motion to stay the *Bessent* preliminary injunction. *AFT* v. *Bessent*, 2025 WL 1023638 (4th

Cir.). Judge Agee and Judge Richardson each wrote opinions concurring in that decision, in which the other joined.

Judge Agee emphasized that all traditional stay factors favored the government, but the government had made a particularly "strong showing that it will succeed on the merits as to standing." *Bessent*, 2025 WL 1023638, at *1; see *id.* at *3. Judge Agee emphasized that the district court's contrary determination—that plaintiffs could demonstrate a concrete Article III injury based on which government employees could access their data—contravened *TransUnion LLC* v. *Ramirez*, 594 U.S. 413 (2021), and circuit precedent. *Bessent*, 2025 WL 1023638, at *1.

Judge Richardson explained that "[a]s a matter of mathematics," the stay analysis favored the government: "Between the four [stay] factors themselves, several threshold jurisdictional questions, and the alleged Privacy Act violation, th[e] case involves several issues that are each potentially dispositive of the appeal." *Bessent*, 2025 WL 1023638, at *3. He explained that the plaintiffs could not show a substantial likelihood of "run[ning] the table" on all of those questions. *Id.* at *5. "First and foremost," he agreed that the plaintiffs "seemingly lack standing." *Id.* at *4. He emphasized the differences between intrusion upon seclusion and the facts alleged here, questioning "whether entries of information in government databases could be part of any plaintiff's seclusion at all." *Ibid.* He further explained that the "harm that might come from granting database access to an additional handful of government employees" seems "different in kind, not just in degree, from the harm inflicted" by snooping "reporters, detectives, and paparazzi." *Ibid.* And he found that the government was likely to prevail on additional issues, including whether the data access decisions constituted final agency action, *id.* at *5; whether the agencies violated the Privacy Act, *id.* at *6; and whether plaintiffs faced irreparable harm, *id.* at *6-*7.

c. Judge King dissented from the panel's decision to grant a stay. *Bessent*, 2025 WL 1023638, at *1, *7. He sought initial en banc consideration of the government's motion for a stay, which the court of appeals denied by a vote of 8-7. *Ibid.* Judge King authored a dissent from denial, which five other judges joined. *Id.* at *7-*10. Judge Berner also issued a dissent from the denial of en banc consideration. *Id.* at *10.

4. Ten days after the court of appeals stayed the *Bessent* injunction, the district court here issued a materially similar injunction, based on essentially the same reasoning. App., *infra*, 21a-174a; see *id.* at 21a n.*. Specifically, the court found that the plaintiff organizations had standing on behalf of their members by analogy to the tort of intrusion upon seclusion, see *id.* at 69a-105a; that the decisions to grant access were final agency action, see *id.* at 114a-125a; that the plaintiffs were likely to succeed on the merits of their Privacy Act and APA (arbitrary and capricious) claims, see *id.* at 132a-158a; that the plaintiffs would suffer irreparable harm absent an injunction, see *id.* at 158a-162a; and that the balance of the equities and the public interest favored an injunction, see *id.* at 163a-166a.

The district court stated that "this case differs markedly" from *Bessent* for three principal reasons, without explaining why those reasons mattered to the legal analysis. App., *infra*, 27a. First, the court found that "virtually from its inception, SSA has been guided by an abiding commitment to the privacy and confidentiality of the personal information entrusted to it by the American people." *Ibid.* Second, given SSA's role in providing benefits to children, "this case involves access to personal information of children." *Id.* at 28a. Third, "this case involves SSA's access, *inter alia*, to extensive medical and mental health records of SSA beneficiaries," *ibid.*—which the court viewed as not "central" in *Bessent, id.* at 98a.

The district court enjoined applicants from granting access to any SSA system of records containing personally identifiable information to DOGE, USDS, the U.S. DOGE Service Temporary Organization, "members of the DOGE Team" at SSA, Elon Musk, Amy Gleason, and "any DOGE Affilate[s]." App., *infra*, 169a. The court ordered the DOGE defendants, SSA DOGE team members, and DOGE affiliates to "disgorge and delete all non-anonym[ous]" personally identifiable information they had obtained from an SSA records system since January 20, 2025, and enjoined them from installing software on SSA devices or accessing or disclosing SSA computer or software code. *Id.* at 170a. Like the TRO, the preliminary injunction allows SSA to provide DOGE Team members with access to certain data and records only if a host of judicially imposed conditions are met. *Id.* at 170a-171a.[3]

5. Applicants timely appealed and sought a stay of the district court's injunction from both that court and the court of appeals. D. Ct. Doc. 149 (Apr. 17, 2025); D. Ct. Doc. 153 (Apr. 18, 2025); 25-1411 C.A. Doc. 6 (Apr. 18, 2025). On April 24, 2025, the district court denied a stay. D. Ct. Doc. 154. On April 30, 2025, the court of appeals granted initial hearing en banc and denied the motion to stay by a vote of 9-6—a two-vote difference from the *Bessent* decision. App., *infra*, 1a-20a.

Judge King filed a concurring opinion, in which six other judges joined. On his view, "DOGE's work could be accomplished" without the access to data that the agency has deemed appropriate and necessary. App., *infra*, 7a. Although Judge King "continue[d] to believe that the stay motion in *Bessent* was worthy of initial en banc consideration and that the stay should not have been granted," he distinguished the

---

[3] While the TRO was in place, applicants notified the district court that, as to four DOGE team members, SSA satisfied the access criteria imposed by the TRO. App., *infra*, 30a. The court construed that filing as a "request to provide access to four DOGE Team members" and denied it as moot as part of the preliminary injunction order. *Id.* at 172a.

cases on the ground that SSA's records include many millions of people, whereas "[t]he *Bessent* injunctive relief, by contrast, was limited to the two million or so plaintiffs." *Id.* at 11a-12a. Judge Wynn and Judge Heytens each issued concurring opinions focused on the decision to consider the stay motion en banc. *Id.* at 13a-15a.

Judge Richardson issued a dissenting opinion in which five other judges joined. He explained that although "this case comes in different clothing, it is the legal twin of" *Bessent*, so that to succeed on their preliminary injunction, the plaintiffs would have to "beat the same long odds as their counterparts" in *Bessent*. *Id.* at 16a-17a. As in that case, "standing is a daunting hurdle all on its own." *Id.* at 17a. Specifically, plaintiffs' analogy to intrusion upon seclusion failed, as "[n]o plaintiff has alleged that they have been the subject of any targeted snooping," or even "that a DOGE-affiliated SSA employee has seen their specific personal information." *Id.* at 20a. He further explained that while "SSA's databases are larger" than the databases at issue in *Bessent*, they contain the same types of sensitive information, and "the jurisdiction and statutory interpretation questions before [the court] presumably come out the same whether [the databases] contain one million rows or one hundred million rows." *Id.* at 18a. Judge Richardson therefore would have "treat[ed] like things alike," and stayed the injunction in this case. *Id.* at 20a.

ARGUMENT

Under Rule 23 of the Rules of this Court and the All Writs Act, 28 U.S.C. 1651, the Court may stay a preliminary injunction entered by a federal district court. See, *e.g.*, *Trump* v. *International Refugee Assistance Project*, 582 U.S. 571 (2017) (per curiam); *Brewer* v. *Landrigan*, 562 U.S. 996 (2010); *Brunner* v. *Ohio Republican Party*, 555 U.S. 5 (2008) (per curiam). To obtain such relief, an applicant must show a likelihood of success on the merits, a reasonable probability of obtaining certiorari, and

a likelihood of irreparable harm. See *Hollingsworth* v. *Perry*, 558 U.S. 183, 190 (2010) (per curiam). In "close cases," the Court will also balance the equities. *Ibid.* Those factors strongly favor a stay of the district court's preliminary injunction in this case.

A. The Government Is Likely To Succeed On The Merits

The district court granted broad injunctive relief to reconfigure the internal workings of a crucial government agency by dictating which agency employees can access agency data and under what conditions. The court did so at the behest of organizations whose members gave the SSA personally identifiable information with the understanding that it would be accessed by government employees in various situations. As the Fourth Circuit recognized on materially similar facts in *Bessent*, the injunction reflects multiple errors. Respondents lack Article III standing because they do not suffer a cognizable harm when certain government employees access their data. Further, the agency's decisions about data access are not final agency action reviewable under the APA. And, even if the case were justiciable, respondents' Privacy Act claims are meritless.

1. Respondents suffer no cognizable Article III injury based on *which* government employees access their data

a. Article III standing is a "bedrock constitutional requirement that this Court has applied to all manner of important disputes." *United States* v. *Texas*, 599 U.S. 670, 675 (2023). It is "built on a single basic idea—the idea of separation of powers." *Ibid.* (citation omitted). The requirement that plaintiffs demonstrate standing "helps safeguard the Judiciary's proper—and properly limited—role in our constitutional system," *id.* at 675-676, by ensuring that federal courts do not become "forums for the ventilation of public grievances" more properly resolved through the democratic process, *Valley Forge Christian Coll.* v. *Americans United for Separation*

of Church & State, Inc., 454 U.S. 464, 473 (1982).

To demonstrate Article III standing, a plaintiff must establish an injury that is both "legally and judicially cognizable," as well as causation and redressability. *Raines* v. *Byrd*, 521 U.S. 811, 819 (1997). The injury requirement includes "that the plaintiff have suffered 'an invasion of a legally protected interest which is . . . concrete and particularized.'" *Ibid.* (citation omitted). As relevant here, an organization may establish standing by showing (in addition to other requirements) the standing of its members. *Hunt* v. *Washington State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977).

b. As six judges recognized below, respondents in this case have not—and cannot—demonstrate that their members have suffered any injury-in-fact. App., *infra*, 19a-20a (Richardson, J., dissenting). To satisfy Article III standing, an injury must be "actual or imminent, not speculative," meaning "the injury must have already occurred or be likely to occur soon." *FDA* v. *Alliance for Hippocratic Med.*, 602 U.S. 367, 381 (2024). The harm must also be "'concrete'—that is, 'real, and not abstract.'" *TransUnion LLC* v. *Ramirez*, 594 U.S. 413, 424 (2021) (quoting *Spokeo, Inc.* v. *Robins*, 578 U.S. 330, 340 (2016)). Although "tangible" harms more readily qualify as concrete injuries, certain intangible harms can also be concrete. *Id.* at 425. "Central to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *Id.* at 417 (quoting *Spokeo*, 578 U.S. at 340-341). And plaintiffs cannot clear the bar by alleging a bare statutory violation. Congress can create "a statutory prohibition or obligation and a cause of action," but it may not override Article III's injury requirement. *Id.* at 426.

Those requirements are fatal to respondents' case. Respondents assert a

purely intangible form of injury—namely, that the disclosure of their personal information to SSA DOGE team members constitutes an invasion of their privacy. That injury is not concrete. Respondents do not contend that their information has been shared with parties outside the government or others likely to misuse their information. To the contrary, SSA DOGE team members—like everyone else at the SSA—are bound by the same legal and ethical restrictions on the disclosure of respondents' information, including the Privacy Act's authorization of criminal penalties for willfully engaging in prohibited disclosures, 5 U.S.C. 552a(i)(1); see 5 U.S.C. 552a(g) (civil remedies against the agency), and the criminal penalties in the Social Security Act, 42 U.S.C. 1306(a).

Respondents' asserted injury thus closely resembles the harms this Court deemed insufficiently concrete in *TransUnion*. There, the Court held that the mere fact that the defendant allegedly maintained inaccurate information about the plaintiffs within the company's files, in violation of a statutory requirement, failed to establish standing. Even though the inaccurate information was quite serious—an alert indicating that the individual's name was a "'potential match'" to a name on a government list of "terrorists, drug traffickers, or other serious criminals"—any harm to the plaintiffs would become concrete only upon publication of the inaccurate information to third parties. *TransUnion*, 594 U.S. at 420, 434.

Here too, the mere fact that the government allegedly committed a statutory violation in allowing certain government employees to access information stored in government databases does not alone demonstrate a concrete harm. Nor does respondents' alleged "distress[]" at the thought of government employees accessing their data suffice. App., *infra*, 20a (Richardson, J., dissenting). Respondents provided their information to the SSA; it is undisputed that the information can lawfully

be accessed by agency employees (and shared outside the agency) for any of the numerous purposes set forth in the Privacy Act and the agencies' System of Record Notices, see 5 U.S.C. 552a(b)(2)-(13); pp. 20-21, *infra*; and the SSA DOGE Team members are subject to the same confidentiality rules and constraints on further dissemination that bind other employees who may access respondents' information.

c. The district court nevertheless held that respondents established an injury-in-fact because respondents' alleged injury purportedly is analogous to the common-law tort of intrusion upon seclusion. App., *infra*, 69a-105a. That conclusion is wrong in several respects.

To start, *TransUnion* requires a "close relationship" between the asserted common-law tort and the alleged statutory violation. 594 U.S. at 425. Although an "exact duplicate" is not required, plaintiffs' contentions must be closely akin to a common-law analogue; even relatively modest distinctions foreclose standing. Thus, *TransUnion* rejected the plaintiffs' fallback argument that the *internal* publication of information to "employees within TransUnion and to * * * vendors" constituted a concrete injury. *Id.* at 434 n.6. Not only was that argument "forfeited," but it was also "unavailing" because "[m]any American courts did not traditionally recognize intra-company disclosures" or disclosures to vendors "as actionable publications for purposes of" the relevant analogue—there, the common-law "tort of defamation." *Ibid.* The cases generally required "that the document was actually read," but that "evidence [was] lacking" in *TransUnion*. *Ibid.*

Here, respondents' novel theory of injury under the Privacy Act bears no resemblance to the traditional tort of invasion upon seclusion—so respondents have not

suffered, and are not in imminent peril of suffering, a concrete, cognizable injury.[4] As the district court acknowledged, App., *infra*, 77a, the Restatement (Second) of Torts defines "intrusion upon seclusion" as "an intentional interference with" a person's "solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man." Restatement (Second) of Torts § 652B(a) (2020) (Restatement). The Restatement provides examples that would meet that high standard, including "physical intrusion into * * * the plaintiff's room in a hotel" or his home; "use of the defendant's senses * * * to oversee or overhear the plaintiff's private affairs"; and "opening [the plaintiff's] private and personal mail [or] searching his safe or his wallet." *Id.* § 652B(b).

Contrary to the district court's determination (App., *infra*, 104a-105a), respondents' alleged injury is "different in kind, not just in degree, from the harm inflicted" by snooping "reporters, detectives, and paparazzi." *Bessent*, 2025 WL 1023638, at *4 (Richardson, J., concurring). It in no way resembles those situations, let alone rises to the level of "highly offensive" conduct. Restatement § 652B(a). SSA personnel here are not surreptitiously invading plaintiffs' hotel rooms or monitoring their private communications. Instead, the SSA undisputedly obtained respondents' personal information legally, and it legally retains that information in data systems that are maintained by, and housed within, the agency.

Simply put, the tort of intrusion upon seclusion "guards against the unease of having one's 'private concerns' specifically targeted by another's 'investigation or ex-

---

[4] In finding that respondents are likely to succeed in demonstrating Article III standing, the district court did not rely on a theory that applicants' internal disclosures create a heightened risk of third-party disclosures. App., *infra*, 75a n.26 (observing that court had rejected such a theory at the TRO stage and incorporating that discussion). As this Court has recognized, any such theory would fail. See, *e.g.*, *Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398, 410-414 (2013).

amination.'" App., *infra*, 19a (Richardson, J., dissenting) (quoting Restatement § 652B cmt. b). "[T]he tort addresses narrow, individualized scrutiny—not general, impersonal oversight." *Ibid.* Yet respondents do not allege "that they have been the subject of any targeted snooping"; nor do they even allege that any "DOGE-affiliated SSA employee has seen their specific personal information." *Id.* at 20a (Richardson, J., dissenting). Respondents' subjective "distress[]" at the knowledge that certain employees have access to SSA databases is an eggshell-plaintiff harm that does not amount to a concrete injury. *Ibid.*; cf. *Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398, 418 (2013) (holding that "self-inflicted injuries are not fairly traceable to the Government's purported activities").

Moreover, when respondents provided their information to the government, they did so on the understanding that the information would routinely be used by agency employees and others within and outside the government to perform the types of activities that the SSA DOGE team members plan to undertake. The agency's System of Records Notice permits even non-government personnel to access data "when they are performing work for us, as authorized by law, and they need access to personally identifiable information (PII) in our records in order to perform their assigned agency functions." See *Privacy Act of 1974; System of Records*, 87 Fed. Reg. 263, 263 (Jan. 4, 2022); *Privacy Act of 1974, as Amended; New and Revised Privacy Act System of Records and Deletion of Obsolete System Records*, 71 Fed. Reg. 1796, 1831 (Jan. 11, 2006); *Privacy Act of 1974, System of Records*, 85 Fed. Reg. 2224, 2226 (Jan. 14, 2020); see also 20 C.F.R. 401.115. Respondents can hardly complain of a concrete injury when they provided their information to a government agency on the understanding that it would be used by agency employees and others to build and maintain computer systems and to investigate improper payments, which is exactly

what the SSA's DOGE team members plan to do.

Indeed, respondents do not dispute that their personal information *can* lawfully be accessed by employees of the agency and shared outside of the agency for any of the numerous purposes set forth in the Privacy Act and the agency's System of Record Notices. See 5 U.S.C. 552a(b)(2)-(13). Nor do respondents dispute that agency employees can and do regularly access their personal information, located in government systems. In practice, respondents would have no reason even to know that a particular employee has accessed their information in the normal course of that employees' duties—as noted above, "[n]o plaintiff has even alleged that a DOGE-affiliated SSA employee has seen their specific personal information." App., *infra*, 20a (Richardson, J., dissenting); see *TransUnion,* 594 U.S. at 438 (certain plaintiffs had not suffered an injury sufficient to support standing where they did not "even *kn*[*o*]*w*" their files contained inaccurate information). Far from constituting a highly objectionable invasion of personal privacy, SSA DOGE team members who access respondents' information are doing the same thing that other agency employees routinely and properly do. That constitutes no injury at all, let alone a cognizable Article III injury.

2. Respondents do not challenge any final agency action

The district court additionally lacked authority to resolve respondents' claim because only "final agency action" is reviewable under the APA. 5 U.S.C. 704. An agency's determination as to which employees may access particular agency data does not qualify. See *Bessent*, 2025 WL 1023638, at *5 (Richardson, J., concurring) (expressing "doubt[] the district court could so definitively find final agency action").

a. It is well settled that not all agency conduct is subject to review under the APA. As this Court has explained, the APA does not permit "general judicial review of [an agency's] day-to-day operations." *Lujan* v. *National Wildlife Fed'n*, 497

U.S. 871, 899 (1990). Nor does the APA authorize agencies to oversee "the common business of managing government programs." *Fund for Animals, Inc.* v. *U.S. Bureau of Land Mgmt.*, 460 F.3d 13, 20 (D.C. Cir. 2006).

Respondents' complaint seeks review of exactly that kind of day-to-day management of agency operations. The supposed "agency action" they identify is a loosely defined series of personnel decisions related to granting individual employees access to agency systems. Respondents contend that the SSA granted access to DOGE team members too quickly and without adequately vetting those employees, providing them with sufficient training, or correctly assessing their need for access to SSA systems. As this Court in *Lujan* explained, such day-to-day decisions and conduct fall outside the APA's ambit. *See Lujan*, 497 U.S. at 899. Lower courts have likewise recognized that courts "are woefully ill-suited * * * to adjudicate" "'attack[s]'" "asking [the judiciary] to improve an agency's performance or operations." *City of New York* v. *United States Dep't of Def.*, 913 F.3d 423, 431 (4th Cir. 2019) (citation omitted). In such cases, "courts would be forced either to enter a disfavored 'obey the law' injunction or to engage in day-to-day oversight of the executive's administrative practices. Both alternatives are foreclosed by the APA, and rightly so." *Ibid.* (citation omitted).

Indeed, respondents' and the district court's understanding of what qualifies as "agency action" would have sweeping and untenable consequences. Agencies make thousands of personnel decisions every day of the type respondents challenge here, whether by creating an e-mail account for an employee, staffing an employee on a particular matter, or ensuring that an employee has the relevant training and credentials to access systems or participate in programs. If courts can review such decisions, virtually every aspect of an agency's internal management of its employees could trigger APA review—a result that no courts have countenanced until now. Far

from identifying relevant precedents for such review, the district court simply stated that the "approval decisions are akin to a binding agency opinion—one that established DOGE's entitlement to access [personally identifiable information] notwithstanding the Agency's customs, practices, policies, and procedures." App., *infra*, 124a. But the fact that an agency decision (in the court's view) differs from prior decisions does not make it a reviewable agency policy.

b. Even if SSA's decisions to grant certain employees access to agency databases qualify as "agency action," they are not "final" for purposes of the APA. Such decisions are not actions through which "rights or obligations have been determined," or from which "legal consequences will flow." *Bennett* v. *Spear*, 520 U.S. 154, 177-178 (1997). Respondents' Amended Complaint fails to demonstrate how providing employees with system access creates any rights, obligations, or legal consequences for respondents. See *United States Army Corps of Eng'rs* v. *Hawkes Co.*, 578 U.S. 590, 597 (2016). There is no final agency action where the challenged act "impose[d] no obligations, prohibitions or restrictions on regulated entities," and "d[id] not subject them to new penalties or enforcement risks." *Sierra Club* v. *EPA*, 955 F.3d 56, 63 (D.C. Cir. 2020). Respondents are not regulated by internal agency decisions to allow new employees access to the agency's systems, nor have they identified any direct legal consequences that arise from those decisions, which may change at any time.

The fact that such decisions could potentially lead to indirect, practical consequences for respondents does not make them final agency action. Adverse effects "accompany many forms of indisputably non-final government action." *Air Brake Sys., Inc.* v. *Mineta*, 357 F.3d 632, 645 (6th Cir. 2004). For example, "[i]nitiating an enforcement proceeding against a company * * * may have a devastating effect on the company's business, but that does not make the agency's action final." *Ibid.* What

matters is that the alleged data access decisions here have no "direct and appreciable legal consequences" for respondents. *California Cmtys. Against Toxics* v. *EPA*, 934 F.3d 627, 640 (D.C. Cir. 2019). That forecloses plaintiffs' APA claim.

In reaching the opposite conclusion, the district court likened this case to *Venetian Casino Resort, L.L.C.* v. *EEOC*, 530 F.3d 925 (2008), in which the D.C. Circuit held that an agency policy to disclose confidential information to third parties constituted final agency action. See App., *infra*, 124a-125a. But there, the court viewed unauthorized third-party disclosures as potentially having direct and immediate consequences for the plaintiffs. See *Venetian Casino Resort*, 530 F.3d at 931. Whatever the merits of that view, review of data contained in internal agency systems by agency employees does not threaten the same harms. Cf. *Hunstein* v. *Preferred Collection & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1240, 1245-1250 (11th Cir. 2022) (en banc) (explaining that without third-party disclosure, claims founded on internal disclosure of data do not state a cognizable injury for standing purposes); see pp. 17-18, *supra* (discussing *TransUnion*'s rejection of an internal-disclosure theory of standing).

3. Respondents' Privacy Act and APA claims fail on the merits

Even were this case justiciable, respondents' claims would fail on the merits. The district court addressed only two of those claims. It found that respondents are likely to succeed on their claims that "SSA's provision to the DOGE Team of access to SSA systems is 'not in accordance with'" law—*i.e.*, the Privacy Act—and that defendants' conduct was arbitrary and capricious, in violation of the APA. App., *infra*, 157a-158a. Each of those holdings was erroneous.

a. While the Privacy Act generally prohibits disclosure of covered records containing personal information absent consent, 5 U.S.C. 552a(b), it contains several exceptions, 5 U.S.C. 552a(b)(1)-(13). As relevant here, the statute expressly author-

izes disclosure to "those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. 552a(b)(1). The disclosure of respondents' records to DOGE team members within the SSA falls comfortably within that authorization.

i. The need exception applies "to intra-agency disclosures." *Britt* v. *Naval Investigative Serv.*, 886 F.2d 544, 547 (3d Cir. 1989). That requirement is met here because the relevant DOGE team members at SSA are employees of the agency for Privacy Act purposes. "For the purpose of" Title 5 of the United States Code—which includes the Privacy Act—"'employee'" means "an officer and an individual who is" first "appointed in the civil service by," *inter alia*, "the President" or "an individual who is an employee under this section." 5 U.S.C. 2105(a)(1)(A) and (D). An employee must also be "engaged in the performance of a Federal function under authority of law or an Executive act," and "subject to the supervision of an individual named by paragraph (1) of this subsection while engaged in the performance of the duties of his position." 5 U.S.C. 2105(a)(2) and (3). The individuals at issue easily satisfy that definition, and the district court did not hold otherwise. See App., *infra*, 138a (assuming that the relevant team members "have 'intra agency' status at SSA").

The employees at issue have a "need" to access the records contained in the relevant systems to perform their official duties. 5 U.S.C. 552a(b)(1). Courts have explained that access is consistent with that requirement if "the official examined the record in connection with the performance of duties assigned to him and [if] he had to do so in order to perform those duties properly." *Bigelow* v. *Department of Def.*, 217 F.3d 875, 877 (D.C. Cir. 2000), cert. denied, 532 U.S. 971 (2001).

That standard is clearly met here. The DOGE team at SSA consists of agency employees who have been tasked by SSA with fulfilling the objective of "modernizing

Federal technology and software to maximize governmental efficiency and productivity." USDS EO § 1; see *id.* § 4. Specifically, the USDS EO has directed the undertaking of a "Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology * * * systems," and it requires agency heads to work with USDS to "promote interoperability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization." *Id.* § 4(a). Consistent with that effort, the USDS EO instructs agency heads "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," and in turn requires USDS to "adhere to rigorous data protection standards." *Id.* § 4(b). A subsequent executive order expanded on that original directive by ordering agency heads to grant specified employees "full and prompt access to all unclassified agency records, data, software systems, and information technology systems * * * for purposes of pursuing Administration priorities related to the identification and elimination of waste, fraud, and abuse." *Stopping Waste, Fraud, and Abuse by Eliminating Information Silos*, 90 Fed. Reg. 13,681, § 3(a) (Mar. 25, 2025) (Data EO).

The USDS and Data EOs thus focus on modernizing the federal government's technology infrastructure and auditing databases to identify waste, fraud, and abuse. The two executive orders in tandem provide agency personnel working pursuant to those EOs with a "need" to access records and systems of records under the Privacy Act in order to do their jobs properly. See *Bigelow*, 217 F.3d at 877. Indeed, it is difficult to imagine how agency personnel seeking to modernize agency systems could do so *without* access to the systems themselves. Such access is necessarily required to assess the state of the systems and to "improve the[ir] quality and efficiency."

USDS EO § 4(a). It is likewise plain that DOGE team members investigating whether the government has made improper expenditures require access to the records detailing the relevant payments. To assess the propriety of any payment, an analyst needs to know the details surrounding that payment, including information about the recipient of that payment, the amount of the payment, the payment's purpose, and so forth. It is hard to fathom how such investigative work could be performed without access to the relevant payment records.

ii. The district court erred in holding that respondents are likely to succeed on their claim that the DOGE team members lack the need for access required by Section 552a(b)(1).

The district court's determination stemmed in significant part from its view that the scope of disclosure in this case is larger than in prior Privacy Act disputes. App., *infra*, 138a (noting that Privacy Act cases "typically involve the disclosure of records concerning a single person or a small number of people"). But it is hardly surprising—much less legally relevant—that employees would "need" to access more records to modernize the government's information systems and detect systemic fraud than would be necessary in a one-off case concerning the government's investigation into, for example, allegations against a particular employee. See, *e.g.*, *Bigelow*, 217 F.3d at 876-877. Here, a limited number of SSA DOGE team members have been granted access to information for specific purposes that require that access. The Privacy Act does not authorize the district court to micromanage that lawful access. Moreover, although the district court purported to exempt non-DOGE activity from its preliminary injunction, see App., *infra*, 172a, the court's reasoning would apparently call into doubt the legality of the SSA's granting of access to the many non-DOGE employees who have had access to the relevant systems for years and who

have been performing tasks substantially similar to the work being performed by DOGE team members. The only apparent difference is that the district court approves of the non-DOGE-related agency employees' activity, but it disapproves of the activities of DOGE. That is the kind of policy judgment that the Constitution vests in the Executive Branch, not district courts.

Much of the district court's analysis focused on whether the applicants demonstrated that, beyond needing access to the records contained in the relevant systems, they *also* needed access to the personal information contained in those records. See App., *infra*, 149a-155a. But it is obvious that SSA employees who are, for example, tasked with investigating whether the government has made improper expenditures would need access to records detailing the relevant payments—including personally identifiable information like the recipient of the payment and its purpose—to determine (among other things) whether duplicative payments were made.

The district court's analysis also fails under the plain text of the Privacy Act. The statute allows employees to access a "record" if they have "a need for the record in the performance of their duties," 5 U.S.C. 552a(b)(1), and it defines "'record'" as "any item, collection, or grouping of information about an individual * * * that contains his name" or other personally identifiable information. 5 U.S.C. 552a(a)(4). In other words, the statutory question is whether the employee needs access to the *record* as a whole—not the personally identifiable information it contains. Moreover, the district court's understanding of the Privacy Act would be entirely unworkable: It would require redaction review of every record and anonymization of certain fields within a record before any employee could do even the most basic tasks required by her job.

The district court's reasoning also fails on its own terms. The administrative record and defendants' declarations explained that although the agency "investigated options for mask[ing] or otherwise protecting" personally identifiable information within records, it had not "identified a solution that enables the necessary analysis to continue at the pace necessary to respond timely to the fraud and improper-payment-related concerns." App., *infra*, 149a (citation and emphasis omitted). The district court found this explanation insufficient, on the theory that "it suggests only that working without" personally identifiable information "may cause the [agency's] work to take longer." *Ibid.* But nothing in the Privacy Act permits the district court to substitute its own judgment regarding the speed required for crucial government work for that of the agency.

b. The district court also erred in holding that respondents are likely to succeed on their claim that applicants acted arbitrarily and capriciously, in violation of the APA. The district court reasoned that "defendants have not provided the Court with a reasonable explanation for why the entire DOGE Team needs full access to the wide swath of data maintained in SSA systems in order to undertake the projects." App., *infra*, 157a. But as already discussed, the government *did* provide such an explanation; and in any event, as Judge Richardson explained in *Bessent*, "it does not stretch the imagination to think that modernizing an agency's software and IT systems would require administrator-level access to those systems, including any internal databases." 2025 WL 1023638, at *6 (Richardson, J., concurring). Once again, the district court's contrary determination simply substitutes its own views of agency best practices for the agency's determination that agency personnel tasked with modernizing the agency's data systems and ferreting out fraud, waste, and abuse need access to those systems.

B. The Remaining Factors Support Relief

In deciding whether to grant emergency relief, this Court also considers whether the underlying issues warrant its review, whether the applicant likely faces irreparable harm, and, in close cases, the balance of equities. See *Hollingsworth*, 558 U.S. at 190. Those factors overwhelmingly support relief here.

1. The issues raised by this case warrant this Court's review

The district court's injunction imposes a significant obstacle to executing one of the President's chief policy initiatives. It relies on a far-fetched reading of the Privacy Act to preclude the SSA—a major federal agency—from effectively complying with the President's direction that the agency modernize federal information systems and identify waste, fraud, and abuse. It does so even though respondents suffer no cognizable injury from a determination as to which specific agency employees may access their records, and even though the day-to-day, internal operations of the SSA do not constitute final agency action. This Court has repeatedly intervened in cases in which lower courts have attempted to micromanage the functioning of the Executive Branch. See, *e.g.*, *OPM* v. *AFGE*, No. 24A904, 2025 WL 1035208 (Apr. 8, 2025) (granting stay of preliminary injunction where plaintiff organizations lacked standing to challenge termination of federal government employees); *Heckler* v. *Lopez*, 463 U.S. 1328, 1329 (1983) (Rehnquist, J., in chambers) (granting stay of district court order requiring Secretary of Health and Human Services "immediately to reinstate benefits to the applicants" and mandating that the Secretary then make certain showings "before terminating benefits"); *Trump* v. *Sierra Club*, 140 S. Ct. 1 (2019) (granting stay of district court order enjoining the Department of Defense from undertaking any border-wall construction using funding the Acting Secretary transferred pursuant to statutory authority); *INS* v. *Legalization Assistance Project*, 510

U.S. 1301, 1305-1306 (1993) (O'Connor, J., in chambers) (granting stay of district court order requiring INS to engage in certain immigration procedures). This case similarly warrants the Court's review.

2. The district court's injunction causes irreparable harm to the Executive Branch

The district court's order also causes irreparable harm to the Executive Branch. More than three months ago, the President signed the USDS EO with the goal of "modernizing Federal technology and software to maximize governmental efficiency and productivity." USDS EO § 1. Yet for much of that time, the district court has blocked SSA from carrying out its mandate while attempting to dictate SSA's internal operations—first in the form of a temporary restraining order, and now via a preliminary injunction. The district court's order impinges on the President's broad authority to direct the federal workforce, to oversee government information systems, and to require agencies to identify fraud, waste, and abuse. It is "an improper intrusion by a federal court into the workings of a coordinate branch of the Government." *Legalization Assistance Project*, 510 U.S. at 1306 (O'Connor, J., in chambers).

3. The balance of equities weighs strongly in favor of the government

The balance of the equities also strongly favors the government. Respondents allege that they face imminent harm from the intra-agency disclosure of information, where employees who view that information are subject to the same confidentiality obligations that apply to other agency employees. As discussed above, see pp. 15-21, *supra*, those allegations do not establish a cognizable injury for Article III standing purposes. Regardless, respondents' abstract objection to government personnel accessing data already in the agency's possession cannot outweigh the government's interest in managing its internal affairs and conducting the review necessary to mod-

ernize government information systems and eliminate fraud, waste, and abuse.

In finding that respondents would suffer irreparable harm absent an injunction, the district court did not suggest that respondents had demonstrated any risk that the SSA defendants or DOGE team members would further disseminate or misuse the relevant data. Rather, the mere fact that certain employees would continue to have access to information respondents' members gave to the SSA was sufficient, in the district court's view, to support the extraordinary relief of a preliminary injunction. App., *infra*, 158a-162a.

That is plainly incorrect. As discussed, the court of appeals in *Bessent*, and three other district courts addressing similar claims, have recognized that similarly situated plaintiffs lack irreparable harm. See *Bessent*, 2025 WL 1023638, at *6-*7 (Richardson, J., concurring); *University of Cal. Student Ass'n* v. *Carter*, No. 25-cv-354, 2025 WL 542586, at *5 (D.D.C. Feb. 17, 2025); *Electronic Privacy Info. Ctr.* v. *U.S. Office of Pers. Mgmt.*, No. 25-cv-255, 2025 WL 580596, at *6-*7 (E.D. Va. Feb. 21, 2025); *Alliance for Retired Ams.* v. *Bessent*, No. 25-cv-313, 2025 WL 740401, at *20-*24 (D.D.C. Mar. 7, 2025). As those courts have explained, "dissemination of information" may constitute "an irreparable injury where, for example, highly sensitive information will be made *public*, or ends up in the hands of someone with no obligation to keep it confidential." *University of Cal. Student Ass'n*, 2025 WL 542586, at *5 (collecting authority); see *Bessent*, 2025 WL 1023638, at *6-*7 (Richardson, J., concurring).

But dissemination of information does not constitute irreparable harm "where the challenged disclosure is not 'public,' but involves individuals obligated to keep it confidential." *University of Cal. Student Ass'n*, 2025 WL 542586, at *5. That is the case here: SSA employees, including DOGE team members, "are obligated to use"

the data "for lawful purposes * * * and to keep it confidential, in accordance with the Privacy Act" and other federal laws. *Id.* at *6; see *Bessent*, 2025 WL 1023638, at *7 (Richardson, J., concurring); *Alliance for Retired Ams.*, 2025 WL 740401, at *21 (explaining that unlawful access does not constitute irreparable injury where the employee is bound to keep information confidential, because, if necessary, "a court can fashion 'adequate * * * corrective relief after the fact") (citation omitted). In short, the balance of the equities strongly favors the government.

C. This Court Should Grant An Administrative Stay

The Solicitor General respectfully requests that this Court grant an administrative stay while it considers the government's submission. The district court's flawed injunction forecloses the Executive Branch from carrying out the pressing priorities of modernizing government information systems and ferreting out fraud, waste, and abuse—all at the behest of plaintiffs who gave their information to the agencies with the knowledge that *other* government employees may access their data. The district court has now blocked these time-sensitive efforts for over a month, without any legal basis for doing so. In these circumstances, an administrative stay is warranted while this Court assesses the government's entitlement to a stay.

CONCLUSION

This Court should stay the district court's preliminary injunction.

Respectfully submitted.

D. John Sauer
Solicitor General

MAY 2025