No. 24A1063

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.

REPLY IN SUPPORT OF APPLICATION FOR A 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

In the Supreme Court of the United States

No. 24A1063

SOCIAL SECURITY ADMINISTRATION, ET AL., APPLICANTS

v.

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

REPLY IN SUPPORT OF APPLICATION FOR A STAY

The district court enjoined particular agency employees—the 11 members of the Social Security Administration (SSA) DOGE team—from accessing data that respondents' members willingly turned over for government use, that other agency employees can unquestionably access, and that the SSA DOGE team will use for purposes that are unquestionably lawful. In doing so, the district court dictated to the Executive Branch which government employees can access which data and even prescribed necessary training, background checks, and paperwork for data access. Appl. App. 170a-171a.

That injunction contravenes this Court's Article III standing precedents, which alone should have precluded any relief. Article III does not open the courthouse doors to plaintiffs who assert supposed injuries based on which government employees access their data for valid, internal government purposes. That injunction also embraces a precedent-defying view of agency action. This Court has long held that the Administrative Procedure Act (APA) is not a vehicle for challenging day-to-day operational decisions, and respondents cannot evade that bar by recharacterizing the

data-access decisions here as a "policy." Finally, that injunction interferes with internal executive-branch functions based on a deeply flawed reading of the Privacy Act. The Executive Branch, not district courts, sets government employees' job responsibilities. District courts should not second-guess whether particular government employees really need particular records to do their jobs.

When district courts attempt to transform themselves into the human-resources department for the Executive Branch, the irreparable harm to the government is clear. And when courts stymie the government's initiatives to modernize badly outdated systems and combat rampant fraud—leaving those initiatives on a litigation track that may halt them for months or years—the irreparable harm is even clearer. Respondents now downplay this dispute as a picayune, fact-bound, Social Security-specific skirmish. *E.g.*, Opp. 11-13. But the issues here are purely legal ones, the injunction thwarts key Executive branch priorities, and the Fourth Circuit took the exceptional step of pursuing initial hearing en banc and issuing four separate opinions—belying respondents' assertion that this is just a mine-run APA dispute. Indeed, the Fourth Circuit inexplicably diverged from its grant of a stay and denial of initial en banc in a mirror-image case, allowing agency-created DOGE teams to access and review records and systems at three other agencies. Yet here, the same en banc court took this case away from the same panel and allowed the district court's sweeping injunction to block the SSA DOGE team from its critical work within SSA. This Court has repeatedly intervened when lower courts have improperly injected themselves into managing the Executive Branch. It should do so again here.

A. The Government Is Likely To Succeed On The Merits

Respondents' claims fail in three independent ways: (1) they lack standing, (2) there is no final agency action, and (3) they allege no violation of the Privacy Act or

APA. "[A]s a matter of mathematics," "the odds that plaintiffs could run the table on all" of those independently fatal issues is exceedingly low. See *American Fed'n of Teachers (AFT)* v. *Bessent*, 2025 WL 1023638, at *3, *5 (4th Cir. Apr. 7, 2025) (Richardson, J., concurring).

1. Respondents lack standing

Respondents concededly have not alleged a "tangible" harm, Opp. 14, and intangible harms can create Article III standing only if they are closely related to traditional common-law harms that supported suit. See Appl. 16-17. Respondents come nowhere close to meeting that standard. They do not allege that their private information will be improperly disclosed outside the government, or even outside SSA. They do not allege any injury from having other SSA employees access their personally identifiable information; indeed, they handed their information over for that very purpose, so they could secure government benefits. Nor do they allege any injury from having government employees look into SSA records writ large for evidence of fraud or improper payments. Their theory of standing is that they will nonetheless suffer personal discomfort if a few other SSA employees—the 11 SSA DOGE team members—can access their information as part of the agency's modernization and antifraud efforts. But hypersensitivity to which government employees can access one's data while performing government functions is not an Article III injury.[1]

---

[1] *United States* v. *Sells Engineering, Inc.*, 463 U.S. 418 (1983), does not hold otherwise. *Sells* noted in a footnote that the Department of Justice Civil Division's ongoing access to grand-jury materials for purposes of a False Claims Act suit was not mooted by the Division's past access. *Id.* at 422 n.6. That footnote does not address standing, and this Court has frequently cautioned against giving "precedential effect" to "drive-by jurisdictional rulin[gs]." *Wilkins* v. *United States*, 598 U.S. 152, 160 (2023) (citation omitted). In any event, the disclosure of confidential grand-jury materials for the Justice Department's use in litigation is quite dissimilar to SSA employees' intra-agency access to SSA data for antifraud functions.

Respondents hang their case (Opp. 15-19) on analogizing their members' discomfort over which particular government employees can access government databases to the common-law tort of intrusion upon seclusion. That analogy is deeply flawed. As respondents agree (Opp. 16), intrusion upon seclusion requires an intentional intrusion upon another's "solitude or seclusion" in a manner that "would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B (1977) (Restatement). But government employees' access to government databases bears no resemblance to hotel break-ins, surreptitious mail-opening, or unconsented-to searches of one's safe—the kinds of intrusion upon "solitude or seclusion" covered by that tort. Appl. 18-19. And government employees accessing government databases to modernize government systems is not "highly offensive to a reasonable person."

Respondents rightly call *TransUnion LLC* v. *Ramirez*, 594 U.S. 413 (2021), "the seminal case" on Article III concreteness, noting that *TransUnion* identified intrusion upon seclusion as a potential common-law analogue. Opp. 15. But they ignore *TransUnion*'s distinction between *internal* publication of information (not an Article III injury) and external publication (an Article III injury). Appl. 17-18 (discussing 594 U.S. at 420, 434 & n.6). Providing data to government employees bound by strict confidentiality obligations is far more akin to internal publication (if that), not to the external surveillance or intrusion on private affairs that could support common-law intrusion-upon-seclusion suits.

Respondents emphasize (Opp. 18) the sensitive nature of the data at issue, like tax and medical records. But respondents offer no authority suggesting that internal disclosure within an organization *authorized* to access the information would have been actionable at common law. For example, the Restatement cites "examining [a] private bank account" as a potential tort. § 652B cmt. b. Yet surely a customer whose

account is audited by his own bank to ensure that he is not a victim of fraud has no claim against bank officials. Likewise, a doctor who directs her nurse to familiarize herself with patients' medical charts is not inviting tort liability—even though medical records are highly sensitive. As Judge Richardson explained, the alleged injury here is "different in kind, not just in degree," from the snooping actionable at common law. *Bessent*, 2025 WL 1023638, at *4; see Appl. 19.

Respondents portray their members as similarly situated to "millions of Americans." Opp. 31. That claim both illustrates the startling breadth of their standing theory and distinguishes any common-law analogue. The tort of intrusion upon seclusion lies when "one's 'private concerns' [are] *specifically* targeted by another's 'investigation or examination.'" Appl. App. 19a (Richardson, J., dissenting) (quoting Restatement § 652B cmt. b) (emphasis added). But, as respondents appear to recognize, Opp. 25-26, SSA DOGE team members do not seek particular individuals' specific information; they seek to modernize SSA systems and identify improper payments, for instance by reviewing swaths of records and flagging unusual payment patterns or other signs of fraud. Appl. 20-21. Any right to be left alone does not include the right to be left alone to defraud the government.

Relatedly, respondents never explain how government employees' access to data that respondents' members provided to the government—including for use in detecting fraud or inefficiencies—could qualify as "highly offensive." Respondents assert that "[t]he government's unauthorized *disclosure*" of their members' records "would be highly offensive to any reasonable person." Opp. 18 (emphasis added). But as respondents elsewhere admit (Opp. 17), "[d]isclosure of private information is a separate tort" that is "irrelevant here." This case involves only internal data access, not disclosure.

Respondents highlight (Opp. 17-18) the district court's supposedly "extensive fact-finding"—an apparent reference to the court's finding that respondents' members expect their data to remain private. *E.g.*, Appl. App. 102a-103a. But that fact-finding does not support the legal analysis needed to compare the allegations in a complaint to the harms actionable at common law. *E.g.*, *TransUnion*, 594 U.S. at 425; *Vermont Agency of Natural Res.* v. *United States ex rel. Stevens*, 529 U.S. 765, 774-777 (2000). Respondents' subjective expectation of privacy has no bearing on whether their theory of harm is analogous to common-law intrusion upon seclusion.

Respondents contend (Opp. 18-19) that Congress's enactment of the Privacy Act elevated the concreteness of the injury, reasoning that Congress effectively treated government employees without a need to know as "intruders." That view of the Privacy Act is incorrect. See pp. 8-10, *infra*. Regardless, "Congress's say-so" cannot make an injury concrete. *TransUnion*, 594 U.S. at 426 (citation omitted). While "Congress may elevate harms that exist in the real world * * * , it may not simply enact an injury into existence." *Ibid.* (internal quotation marks omitted).

Respondents' theory would confer on every American a cognizable "right to privacy" against disfavored government employees accessing any given government record, thereby implausibly granting standing to "millions of Americans." Opp. 19-20, 31. The only thing that sets respondents apart is their members' apparent antipathy to having SSA DOGE team members—but not other SSA employees—access their data. Some other plaintiffs might object to access for SSA accountants, SSA lawyers, SSA political appointees, or SSA employees from the wrong political party, on the theory that those employees are unqualified, inadequately trained, or untrustworthy. That open-ended theory rests on a hitherto unrecognized right to micromanage government information-technology decisions, not the narrow common-law right against

intrusion upon seclusion. Recognizing an actionable injury here would vitiate *TransUnion*'s demand for a close common-law analogue and open the floodgates to standing based on all sorts of idiosyncratic data-access concerns.

2. Respondents do not challenge final agency action

Respondents' claims independently fail because "day-to-day [agency] operations" fall outside the APA. See *Lujan* v. *National Wildlife Fed'n*, 497 U.S. 871, 899 (1990). Respondents acknowledge that rule and disclaim (Opp. 21) any challenge to individual SSA personnel decisions. But they attempt to end-run the rule by purporting to challenge (Opp. 22) an implicit "wholesale change to [SSA's] prior access policies." Respondents offer no way to police the boundaries between a supposed "policy" and ongoing day-to-day operations. As this Court held in *Lujan*, that sort of challenge involves no "agency action" under the APA, let alone final agency action.

a. A series of unreviewable day-to-day agency decisions does not become reviewable agency action just because plaintiffs can identify a common thread linking them. In *Lujan*, this Court rejected a challenge to the government's purported "land withdrawal review program"—in actuality, a series of small-bore agency land-use decisions. 497 U.S. at 890. Even though the plaintiffs alleged recurrent legal violations by the agency, those "day-to-day operations" fell outside the APA. *Id.* at 891, 899.

Similarly, respondents attack (Opp. 21) a supposed "polic[y]" of giving "the DOGE Team" "expansive access to SSA systems of records (without signed detail agreements, adequate training, completed background investigations, executive work forms, or actual or articulated need)." But that purported "policy" is merely a series of personnel decisions in which respondents allege recurrent defects. If that is agency action, so would be the routine "failure to revise land use plans in proper fashion"—the theory *Lujan* rejected. 497 U.S. at 891.

Respondents' theory would allow virtually any agency decision to be transformed into the subject of an APA suit by alleging some global "policy" divined from agency practice that deviates from a statutory requirement or the APA. Respondents disclaim seeking review of day-to-day SSA operations. But they never explain how to differentiate between the "decision" to give "any member of the DOGE Team" access—in their view, an actionable policy, Opp. 21—and giving one, two, or eleven DOGE team members access in identical circumstances. Given the thousands of personnel decisions that agencies make every day, respondents' theory risks turning many mundane decisions into APA suits.

b. Respondents also flunk the APA's requirement that agency action be "final" because no "legal consequences" "flow" from SSA DOGE team members' data access. See *Bennett* v. *Spear*, 520 U.S. 154, 178 (1997) (citation omitted). Respondents assert that the "disclosure of [confidential] information" affects legal rights. Opp. 23 (discussing *Chrysler Corp.* v. *Brown*, 441 U.S. 281 (1979)). And respondents press (Opp. 23) their analogy to *Venetian Casino Resort, L.L.C.* v. *EEOC*, 530 F.3d 925 (2008), where the D.C. Circuit found final agency action in the EEOC's "policy of disclosing [employers'] confidential information" to potential discrimination plaintiffs or competitors "without notice." *Id.* at 927, 931. But again, this case involves only data access, not disclosure, much less disclosure to a potential litigation opponent or competitor. See p. 5, *supra*. And changes in internal agency practice over whether employees must "sign[] detail agreements" or complete "executive work forms" (Opp. 21) do not carry legal consequences for regulated parties.

3. Respondents' claims fail on the merits

Privacy Act. The Privacy Act expressly authorizes agency employees "who have a need for the record in the performance of their duties" to access a record,

among many other exceptions for access. 5 U.S.C. 552a(b)(1). The district court did not dispute that SSA DOGE team members are SSA employees. Appl. App. 138a. And employees tasked with "modernizing Federal technology and software to maximize governmental efficiency and productivity" logically need access to the technology and software they are seeking to modernize. Exec. Order 14,158, § 1, 90 Fed. Reg. 8441 (Jan. 20, 2025) (USDS EO); see Appl. 25-27.

Respondents all but ignore that common-sense proposition, instead demanding an absurd and infeasible record-by-record, employee-by-employee showing to justify access. But the Privacy Act "need" standard is simply "whether the official examined the record in connection with the performance of duties assigned to him and whether 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). It should hardly be surprising that employees with broader job responsibilities will need broader access to do their jobs. As the concurring judges below pointed out, a "few" SSA employees have access that equals or "exceed[s] that allowed" to the SSA DOGE team. Appl. App. 7a (King, J., concurring); see D. Ct. Doc. 36-1, ¶ 20 (Declaration of SSA Chief Information Officer Michael Russo). In any computer system, someone needs high-level administrator access to keep the system running, manage updates, and make improvements. Yet no one thinks information-technology specialists must justify their access on a document-by-document, line-by-line basis. The need for access tracks the job responsibility, and respondents cannot rewrite the Privacy Act to provide otherwise based on a policy objection to the President's antifraud and modernizing mission for the U.S. DOGE Service (USDS).

Underscoring the SSA DOGE team's need for access, the President directed that agency heads grant "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." Exec. Order 14,243, § 3(a), 90 Fed. Reg. 13,681 (Mar. 25, 2025). Respondents object (Opp. 26) that "Executive Orders cannot supersede a duly enacted statute." Accord Opp. 27 n.4, 28. But the Privacy Act asks whether the agency officials "have a need for the record in the performance of their duties." 5 U.S.C. 552a(b)(1). To identify what those duties are, courts naturally look at the Executive Branch's job descriptions. And modernizing government-wide information technology and combatting fraud are duties that necessarily require broad access.

Respondents question (Opp. 25-26) why SSA DOGE team members cannot make do with anonymized records. As then-Acting Commissioner Dudek explained, "data anonymization is not feasible" and is "impracticable" given both the nature of the team's work and the structure of SSA's databases. D. Ct. Doc. 62-1, ¶¶ 7, 9-11 (Mar. 27, 2025); D. Ct. Doc. 80-1, ¶¶ 4-6 (Apr. 1, 2025). For instance, a birthdate of 1900 can be telltale evidence that an individual is probably deceased and should not still receive Social Security payments, while 15 names using the same social security number may also point to a problem.

Moreover, respondents' demand for anonymization depends on the erroneous premise that every piece of personally identifiable information is itself a "record" covered by the Privacy Act. But the statutory text instead defines a record as "any item, collection, or grouping of information about an individual that is maintained by an agency * * * and that contains" personally identifiable information. 5 U.S.C. 552a(a)(4). In other words, a record *contains* personally identifiable information; the personally identifiable information is not itself the record. Respondents cite legislative history quoted in 50-year-old agency guidance that describes Congress's "intent

that a record can include as little as one descriptive item about an individual." 40 Fed. Reg. 28,951, 28,952 (July 9, 1975) (quoting 120 Cong Rec. 40,883 (1974)). But even if a record *can* include a single descriptive item, the SSA records at issue here undisputedly contain many pieces of information. The Privacy Act requires only that the officials have a need for the record as a whole.

At bottom, respondents insist (Opp. 27-28) that applicants must show that the employees literally "need" the records such that work would be physically impossible without them. Respondents thus dismiss (Opp. 27) the idea that the ability to "merely be able to work faster" can establish need. Respondents cite no authority besides the decision below adopting that crabbed understanding of "need." Just as modern-day lawyers "need" internet access notwithstanding the existence of hard-copy case reports, SSA DOGE team members "need" access to nonanonymized data to do their jobs, even if cumbersome, time-consuming alternatives might exist. Any contrary reading would grind the federal government to a halt, forcing courts to parse whether every employee could potentially make do without individual records.

Respondents also press (Opp. 28-29) an argument not reached below: that SSA DOGE team members are supposedly employees of USDS, not SSA, because DOGE teams "coordinate their work with USDS." USDS EO § 3(c). But as that same subsection makes clear, DOGE teams are "establish[ed] *within* their respective Agencies" by "each Agency Head." *Ibid.* (emphasis added). In other words, the SSA DOGE team was established by the Acting Commissioner of Social Security and sits within SSA. DOGE teams coordinate their work with USDS to ensure that all DOGE teams are aligned in "implementing the President's DOGE Agenda." *Ibid.* That coordination obligation does not make the SSA DOGE team any less a part of SSA.

APA. Respondents' arbitrary and capricious claim asserts (Opp. 31) that SSA

has undertaken a "sea change" in granting access to the SSA DOGE team "without acknowledging or considering the risks posed by unauthorized DOGE Team access." As explained, far from being "unauthorized," the SSA DOGE team's access lawfully implements the President's Executive Orders so that agency employees can access the data needed to combat waste, fraud, and abuse. See pp. 9-10, *supra*.

Respondents also assert (Opp. 31) that SSA discarded Americans' reliance interests "in SSA continuing to preserve the confidence of their information." The district court rightly did not espouse that theory. See Appl. App. 157a-158a. SSA DOGE team members are bound by the same legal and ethical confidentiality obligations governing everyone at SSA. Appl. 17.

B. The Remaining Factors Support Relief

Certworthiness. Respondents do not dispute that this Court often intervenes when, as here, lower courts attempt to wrest control of internal executive-branch functions. Appl. 30-31. Respondents deem (Opp. 11-13) review inappropriate because there is no circuit split and other DOGE data-access cases are percolating in the lower courts. But this case is already on an extraordinary track: The Fourth Circuit granted initial hearing en banc while simultaneously denying initial en banc in this case's "legal twin," *AFT*, 2025 WL 1023638. Appl. App. 16a (Richardson, J., dissenting). That two-vote flip inexplicably grants DOGE team members full access to combat waste, fraud, and abuse at the Department of Education, the Department of Treasury, and the Office of Personnel Management, but not at SSA. Even the judges voting to deny a stay recognized the "vastly greater stakes" justifying initial en banc review. Appl. App. 11a (King, J., concurring). Respondents point out (Opp. 12) that other DOGE data-access cases are still proceeding, but the sheer number of cases and disparate results even within the Fourth Circuit only underscore the importance. An

en banc Fourth Circuit decision stopping a major administration priority in its tracks plainly warrants review—particularly when the injunction here rests on deeply flawed standing and merits theories.

Irreparable Harm. The government suffers irreparable injury "[a]ny time" it is "enjoined by a court from effectuating statutes enacted by representatives of [the] people." *Maryland* v. *King*, 567 U.S. 1301, 1303 (2012) (Roberts, C.J., in chambers); accord *Bessent*, 2025 WL 1023638, at *3 (Agee, J., concurring). While this case involves an executive order, not a statute, the harm is no different: the district court has blocked one of the Administration's key priorities. That inflicts ongoing harm on the Executive Branch's efforts to root out fraud and modernize outdated systems and prevents SSA's DOGE team from thoroughly reviewing SSA—an agency with one of the largest documented histories of improper payments. Appl. 6-7.

The district court's preliminary injunction imposes further irreparable harm by micromanaging how the Executive Branch can combat fraud within its own systems—requiring the Executive to use personnel the district court approves, pursuant to processes that court selects. Respondents note (Opp. 32-34) that the district court left the door ajar to case-by-case access for individuals meeting training criteria who provide a "detailed," record-by-record explanation of need that the district court reserves the right to review. Appl. App. 171a. But that proposal is the problem, not the fix. The notion that a single district court would superintend agency officials' completion of onboarding paperwork and training modules and then assess their need for every single record required to do their job only underscores the interbranch intrusion. Moreover, the one time the government attempted to use that avenue at the TRO phase, the district court inexplicably denied the request as "moot." *Id.* at 172a.

Relatedly, respondents downplay (Opp. 34-36) the significance of the district

court's requirement that the SSA DOGE team use anonymized data. As noted, Acting Commissioner Dudek deemed that approach infeasible. See p. 10, *supra*. Anonymization would require "highly complex technical and statistical skill" and "large amounts of employee and system resources to complete." D. Ct. Doc. 80-1, ¶ 5.[2] It would be perverse to require employees tasked with combating waste and inefficiency to undertake a highly wasteful and inefficient process just to do their jobs—and doing so would compromise the whole effort.

Those harms are irreparable without the need for the government to produce "record" "evidence" of how, for example, the President's inability to "direct[] the workforce" is an irreparable harm. Contra Opp. 35. Nor is the argument a "new development." Contra Opp. 34. DOGE's mission has always been to "moderniz[e] Federal technology and software to maximize governmental efficiency and productivity," including by ferreting out fraud. USDS EO § 1; accord, *e.g.*, Gov't C.A. Mot. for Stay 6-7 ("DOGE team members employed by the SSA * * * need to perform their vital work of modernizing and improving the systems, while also rooting out fraud and waste within government programs.").

Respondents present (Opp. 36) "waiting for a decision from the Fourth Circuit" as a minor inconvenience. But respondents' brief is not due until July 9, 2025; oral argument is not yet scheduled; and the Fourth Circuit will presumably take yet further months to issue an opinion. Opp. App. 7a. By the time this Court might hear the merits, October Term 2026 could be well under way. The Fourth Circuit's stay denial thus raises the prospect that a day-one administration priority could remain

---

[2] Respondents mischaracterize (Opp. 36) Acting Commissioner Dudek as elsewhere endorsing anonymized data. The cited declaration describes how a single SSA DOGE employee will use existing anonymized data to identify anomalous cases that require follow up. D. Ct. Doc. 74-1, ¶ 8. That employee will "need[] access to discrete individual data" once anomalies are identified. *Ibid.*

blocked at SSA into 2027, more than two years after inauguration day.

Balance of the Equities. On the other side of the ledger, respondents vastly overstate their interest in preventing government employees from accessing respondents' members' government data. Respondents do not dispute that DOGE SSA personnel are subject to the same strict confidentiality standards as other SSA employees. Appl. 31-32. And respondents make no allegation that the SSA DOGE team's access will increase the risk of public disclosure. Appl. 32. Again, respondents' entire theory of injury (Opp. 37) is that their members experience a subjective "invasion of privacy" and personal discomfort from that access. But the disclosure of information to "individuals obligated to keep it confidential" does not establish irreparable injury. *University of Cal. Student Ass'n* v. *Carter*, No. 25-cv-354, 2025 WL 542586, at *5 (D.D.C. Feb. 17, 2025). Moreover, respondents could recover for any Privacy Act violations on the back end via damages, 5 U.S.C. 552a(g)(4), without any need for an injunction. While respondents dismiss damages as insufficient (Opp. 37), they do not explain why that standard tort-law remedy would not remedy their asserted injury. Given respondents' lack of irreparable harm—or any cognizable harm at all—the public interest strongly favors a stay.

* * * * *

For the foregoing reasons and those stated in the government's application, this Court should stay the district court's preliminary injunction.

Respectfully submitted.

D. JOHN SAUER
Solicitor General

MAY 2025