UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CENTER FOR TAXPAYER RIGHTS et al.,

Plaintiffs,

v.

INTERNAL REVENUE SERVICE et al.,

Defendants.

Civil Action No. 25-cv-457-CKK

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR STAY UNDER 5 U.S.C. § 705 OR, IN THE ALTERNATIVE, FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

The IRS holds taxpayer information on virtually every American. It is among the most sensitive and confidential personal information in government systems. As a result, and in response to Nixon-era abuses, Congress enacted stringent privacy protections in the Tax Reform Act of 1976, and for decades IRS policy has been to carefully guard the confidentiality of taxpayer data. Now, however, the IRS has adopted a new policy ("the Data Policy") to widely share taxpayers' sensitive data. Defendants' new, unannounced, and unexplained Data Policy is unlawful and is already causing irreparable harm to Plaintiffs and others. Plaintiffs ask the Court to stop it.

In recent days, Defendants have begun executing this Data Policy at mass scale. During the week of August 4, 2025, the IRS shared tens of thousands of taxpayers' data within days of receiving an Immigration and Customs Enforcement ("ICE") request for the addresses of more than 1 million taxpayers, purportedly under a narrow exception to taxpayer confidentiality laws. But that exception, which allows the IRS to provide information for specific criminal investigations and proceedings, does not apply to the IRS's bulk disclosure of sensitive information, and ICE's request failed on its face to comply with the laws protecting taxpayer confidentiality. It is entirely implausible that ICE is conducting *bona fide* criminal investigations of over 1 million people or that it seeks home addresses for use in preparation for judicial or administrative proceedings or investigation that may lead to such proceedings, as the law requires. Rather, as the White House said in July, this data sharing is "part of President Trump's promise to carry out the mass deportation of criminal illegal aliens"—a *civil* immigration enforcement effort that is not a legal basis for ICE to request or receive confidential taxpayer information from the IRS.

Nonetheless, the IRS disregarded its statutory obligations to protect the confidentiality of taxpayer information and responded with home addresses for the taxpayers it was able to locate in its system. Thus, in just one week, the IRS disseminated as much taxpayer data under this inapposite criminal proceeding provision to ICE as it had previously shared in a single year with *all* federal law enforcement agencies, which have never before included ICE. And yet, because the IRS was able to find matches in its system for less than 5% of the names ICE requested, this unprecedented and unlawful disclosure of taxpayer data was apparently not enough for this Administration. The new IRS Commissioner was consequently fired, to join the ranks of the five Acting Commissioners and dozens of senior privacy, legal, and IT leaders pushed out of the agency in the last 7 months after raising objections to the Administration's reckless handling and unlawful disclosures of confidential taxpayer data.

The IRS's recent implementation of the Data Policy at mass scale to share unprecedented quantities of taxpayer data with ICE at breakneck speed illustrates the unlawful and arbitrary nature of the Data Policy. In section 6103(i)(2) of the Internal Revenue Code, Congress provided a host of specific requirements to govern requests for information relevant to criminal matters—which the IRS has long interpreted *not* to permit disclosures for purposes of obtaining address information—and the IRS has historically carefully responded to these requests on a case-by-case basis. But in a reversal of that policy and practice, the IRS has now responded to at least one *en masse* request from ICE seeking the data of as many as 1.23 million people, on a turnaround time of just days. It is neither plausible nor possible that the IRS is ensuring that this data will be shared only with specific law enforcement officers "directly and personally engaged" in specific investigations of specific non-tax criminal statutes, as required by the law, or that the IRS is carefully evaluating each request. And the IRS has provided no explanation, let alone the

reasoned explanation required by the Administrative Procedure Act, for its abrupt reversal of privacy protections to allow this to happen.

While the Data Policy challenged in this action is not limited to the IRS's data sharing with ICE, this emergency Motion seeks relief with respect to this narrower implementation of the Policy, which is confirmed to be already occurring. Defendants' initiation of mass data sharing with ICE under the Data Policy is causing and threatens irreparable harm to Plaintiffs and their members and clients. This sharing is irreversibly harming Plaintiff Center for Taxpayer Rights' ("CTR" or "the Center") ability to provide the education and representation services for immigrants who speak English as a second language, as well as its efforts to promote trust and engagement in the tax system, obstructing the organization from fulfilling its core mission and statutory responsibilities as a Low Income Taxpayer Clinic. CTR's clients and Plaintiff Main Street Alliance's ("MSA") members also include immigrants and taxpayers with immigrant family members, whose data may already have been unlawfully shared with ICE or who are at imminent risk of having their data unlawfully shared with ICE, and who are already suffering concrete and irreparable injuries as a result. Members of Plaintiffs National Federation of Federal Employees, IAM AFL-CIO ("NFFE") and Communication Workers of America, AFL-CIO ("CWA") similarly face heightened risks that their data will be disclosed. Plaintiffs respectfully request that this Court stay or preliminarily set aside Defendants' sharing of address information with ICE under the Data Policy and return or destroy any such information already disclosed to prevent further irreparable harm before the Court can resolve this action on the merits.

BACKGROUND

Longstanding IRS policy strictly controlled the dissemination of taxpayer information within the federal government, in conformance with protections codified in 26 U.S.C. § 6103. In

an unannounced reversal of this policy, Defendants have now effected a new IRS Data Policy that prioritizes consolidation of protected data and free sharing across the federal government. The Administration has pressed forward with this change over the objections of IRS leadership and long-serving senior executive service IT staff, such that scores of senior IRS officials have been fired, put on administrative leave, or quit.

Defendants are now implementing data sharing under the new Data Policy at scale. In recent years, the IRS has shared between 40,000 to 70,000 individuals' tax information with law enforcement each year for non-tax criminal matters. That reflects the total number of disclosures across all federal law enforcement agencies, none of which were to ICE. Under the new Data Policy, in the first week of August alone, the IRS reportedly shared approximately 60,000 individuals' return information with ICE, within days of receiving an *en masse* request,[1] despite a stated requirement that the IRS "review each request for completeness and validity."[2] This sharing was purportedly authorized under Section 6103's provisions for the sharing of information with law enforcement officers who "are personally and directly engaged" in a criminal investigation or proceeding under a specifically identified criminal statute. 26 U.S.C. § 6103(i)(1, 2). In light of the irreparable harms caused and threatened by this mass sharing, Plaintiffs filed this motion for emergency relief.

[1] Rene Marsh, *IRS begins sharing sensitive taxpayer data with immigration authorities to find undocumented migrants*, CNN (Aug. 8, 2025), https://perma.cc/24KK-QZMB (Ex. 1).
[2] *Mem. of Understanding Between IRS and ICE*, at 5.B https://perma.cc/BHH8-ZQXM (Ex. 4).

I. The IRS Has Long Stringently Protected Taxpayer Information, As a Matter of Law and Policy.

The IRS collects and maintains the sensitive and confidential data of more than 150 million individual taxpayers and millions more businesses.[3] This data includes social security numbers ("SSNs"), individual taxpayer identification numbers ("ITINs"), addresses, bank account and employment information, medical expense information, and confidential business information. *See* 26 U.S.C. § 6103(b)(2). In the wake of abuses by the Nixon Administration, including efforts to use confidential information to target political enemies, Congress passed the Tax Reform Act of 1976 (codified in the Internal Revenue Code of Title 26), which implemented significantly more protective controls and limitations on the sharing of IRS tax information within the federal government.[4] The IRS policy manual implements these statutory requirements with detailed requirements and limitations on how taxpayer information may be accessed and disclosed.[5] Pursuant to these laws and policies, the IRS has stringently protected taxpayer information, even from sharing within the federal government, for decades.

---

[3] *See* IRS, *2024 Internal Revenue Service Data Book*, https://perma.cc/XG7C-RKZ5.

[4] Taxpayer Advoc. Serv., *National Taxpayer Advocate: 2003 Annual Report to Congress* at 245 (Dec. 31, 2003), https://perma.cc/T6ZD-Q6VL ("Taxpayer Advocate Report") (explaining that the Act significantly limited "the rules governing the availability of tax information to Federal agencies for purposes of nontax criminal cases," and that the Senate Finance Committee determined that an individual's tax information is "entitled to essentially the same degree of privacy as those private papers maintained in his home").

[5] *See* Internal Revenue Manual § 10.5.2, *Privacy Compliance and Assurance (PCA) Program*, IRS (Jan. 27, 2020), https://perma.cc/JP7T-9WEX ("IRM"); IRM § 9.3.1, *Disclosure*, IRS (Dec. 19, 2024), https://perma.cc/4VL8-75KK. The Privacy Act was enacted two years earlier to protect sensitive personal data held by all federal agencies across the federal government. 5 U.S.C. § 552a; Sam Berger & Alex Tausanovitch, *Lessons From Watergate*, Ctr. for Am. Progress (July 30, 2018), https://perma.cc/M8XB-NDF8. Plaintiffs have pled that the Data Policy is contrary to both the Privacy Act and the Internal Revenue Code, but here move for relief solely on the basis of their APA contrary to law claim concerning the Internal Revenue Code as well as APA arbitrary and capricious claims.

A. Section 6103 Explicitly Limits Sharing of Taxpayer Data Within the Federal Government, Including When Requested for Purported Criminal Investigations.

Section 6103 of the Internal Revenue Code requires that Plaintiffs' members' "[r]eturns and return information shall be confidential." 26 U.S.C. § 6103(a). It prohibits any inspection or disclosure of that information unless the requirements for one of the listed exceptions are met. *Id*. And its exceptions are either connected with tax administration or permit disclosure to other federal agencies only for specific, limited purposes. *See id.* §§ 6103(i), (j), and (l). Treasury Department officers and employees can only be granted access to inspect or disclose tax information where their "official duties require such inspection or disclosure for tax administration purposes." *Id*. § 6103(h)(1). And 26 U.S.C. § 7213A prohibits IRS employees and officers from inspecting returns or return information without authorization.

Section 6103 contains specific requirements for the sharing of taxpayer data when requested for criminal investigations conducted by other agencies. Section 6103(i)(2) provides that "return information" may be disclosed to "officers and employees of [a requesting federal] agency who are *personally and directly* engaged in" an investigation or proceeding "of a specifically designated criminal statute." *Id*. § 6103(i)(2)(A); (i)(1)(A) (emphasis added). To meet the requirements for sharing return information in response to a request under this provision, the requesting agency must provide the taxpayer's name and address, the taxable periods to which the requested return information relates, the specific criminal statutory authority under which the investigation or proceeding is being conducted, and the "specific reason or reasons" why disclosure of return information is relevant to the criminal investigation or proceeding. *Id*. § 6103(i)(2)(B). Further, certain disclosures require a court order, including disclosures made for the purpose of locating an individual. *See id*. § 6103(i)(1)(A), (i)(4), (i)(5).

B. IRS Policy has Long Stringently Protected Taxpayer Data.

In conformance with Section 6103, the IRS has long restricted how personal and business information can be shared within and outside of the agency.[6] *See* Declaration of John Koskinen, Ex. 11 ("Koskinen Decl.") ¶ 8–12. For example, interagency sharing or combining of taxpayer information has been permitted "only where the agency can demonstrate, using established criteria, a need for the information that clearly outweighs taxpayer privacy interests and concerns about the effect on voluntary tax compliance."[7] Therefore, "if IRS [taxpayer] data is to be provided at all, the IRS should be the last stop—not the first—for information for purposes unrelated to tax administration."[8] The IRS's Internal Revenue Manual, therefore, requires employees to complete rigorous steps prior to disclosing any tax information under each provision of Sec. 6103.[9]

The combination of the IRS's adherence to statutory requirements, compliance with the IRS policy manual, and prioritization and implementation of privacy-protective practices has established a longstanding policy (the "Privacy Policy") that has spanned decades. The Privacy Policy was grounded in key principles, integrated into data-sharing and data-access decisions made by IRS leadership, based on statutory requirements and longstanding agency judgment.

---

[6] *See* IRM §§ 10.5.2.1.1, *Background, & 10.5.2.1.3, Responsibilities,* IRS (Jan. 27, 2020), *https://perma.cc/JP7T-9WEX*; IRM §§ 11.3.28.1.1, *Background*, https://perma.cc/HY8W-QPJG, IRS (April 17, 2025) ("Congress decided that federal law enforcement officials should not have easier access to information about a taxpayer maintained by the IRS than they would have if they sought to compel the production of that information from the taxpayer themselves").

[7] Dep't of Treasury, *Report to the Congress on Scope and Use of Taxpayer Confidentiality and Disclosure Provisions, Vol. I: Study of General Provisions* at 9 (Oct. 2000), https://perma.cc/2LC2-M9F5.

[8] *Id*. at 34.

[9] *See generally* IRM § 11.3.28, *Disclosure to Federal Agencies for Administration of Non-Tax Criminal Laws*, IRS (Apr. 21, 2025), https://perma.cc/J7Z3-8FVS.

These included: prioritizing public trust;[10] protecting taxpayer information within the IRS *and* at agencies that receive taxpayer information, including by segregating taxpayer information across databases;[11] evaluating disclosures of taxpayer information on a case-by-case basis;[12] and disclosing IRS data only when other data cannot suffice.[13] This Privacy Policy has been well understood by the IRS and the public alike. For decades, the IRS has assured the American public that their data in its possession is confidential. As a 2013 publication for government employees put it: "The General Rule - Tax Information Is Confidential!"[14]

C. The IRS's Longstanding Privacy Policy Extended to Requests for Return Information for Use in Criminal Investigations.

As the IRS itself states in its Manual, in enacting 6103(i), "Congress determined that federal law enforcement officials should not have easier access to information about a taxpayer maintained by the IRS than they would have if they sought to compel the production of that

[10] *See, e.g.*, IRS, Tax Information Security Guidelines at 23, https://perma.cc/9EEP-KZ6D ("The IRS must administer the disclosure provisions of the Internal Revenue Code (IRC) according to the spirit and intent of these laws, ever mindful of the public trust."); *Gardner v. United States*, 213 F.3d 735, 738 (D.C. Cir. 2000) ("This general ban on disclosure provides essential protection for the taxpayer…The assurance of privacy secured by § 6103 is fundamental to a tax system that relies upon self-reporting."); *see also* Jacob Bogage & Shannon Najmabadi, *Acting IRS chief to quit over deal to share data with immigration authorities*, Wash. Post (Apr. 9, 2025), https://perma.cc/D7XE-7FDD (explaining "the tax agency's longtime guarantee that taxpayers suspected of being in the country illegally wouldn't have their information turned over to immigration enforcement").

[11] Hannah Natanson, *et al.*, *DOGE aims to pool federal data, putting personal information at risk*, Wash. Post (May 7, 2025), https://perma.cc/9JCK-9K4W ("'Separation and segmentation is one of the core principles in sound cybersecurity.'"); *see*, *e.g.*, IRS, *Tax Information Security Guidelines*, https://perma.cc/9EEP-KZ6D.

[12] *See, e.g.*, IRM § 11.3.22.2, *Disclosure to certain Federal Officers and Employees for Tax Administration Purposes under IRC 6103(h)*, IRS (Aug. 9, 2024), https://perma.cc/5ZN4-NM4E.

[13] *See, supra,* n.7, at 34.

[14] IRS, *Protecting Federal Tax Information for Government Employees*, Publication 4761 (Rev. 9-2013), https://perma.cc/5KYH-MNYB.

information from the taxpayer themselves."[15] The agency has judged that 6103(i) "establishes the general rule that a federal agency enforcing a non-tax criminal law must obtain court approval to obtain a return or return information."[16] Under the sub-provision 6103(i)(2), which creates a limited exception for which court approval is not required, Congress and the IRS have imposed numerous other safeguards, permitting disclosures of only very limited pieces of information and requiring the requesting agency to include a specific justifications for the information. For example, prior to April 17, 2025—when the Manual was updated—it directed IRS employees processing a Section 6103(i)(2) request to, *inter alia*, "analyze [the] request," "discuss" with the requesting law enforcement officer the "time frames and specific information requested," and "analyze" the requested return information "for potential redactions."[17]

II. Defendants Have Radically Shifted the IRS's Data Policy and are Rapidly Implementing it Through Sharing Data with DHS.

In this Administration, Defendants abruptly changed the IRS's longstanding Privacy Policy and implemented a permissive data-sharing policy that prioritizes the consolidation and inter-agency sharing of sensitive taxpayer information in the IRS's custody. Under this new Data Policy, earlier this month Defendants began sharing IRS data *en masse,* through automated means, with ICE pursuant to an agreement with DHS, quickly responding to ICE requests for taxpayer information concerning more than a million individuals in one fell swoop.

---

[15] IRM § 11.3.28.1.1, *supra* n.6.
[16] *Id*.
[17] IRM § 11.3.28, Exhibit 11.3.28-2 *Processing IRC 6103(i)(2) Requests*, IRS (Aug. 11, 2023), https://web.archive.org/web/20250403125859/https://www.irs.gov/irm/part11/irm_11-003-028#idm139635074069120 (capture date April 3, 2025). These processing instructions were materially changed in the April 2025 updates, removing many of these cautions and safeguards. *Compare with* IRM § 11.3.41, Exhibit 11.3.41-6 *IRC 6103(i)(2) Case Processing Checklist*, IRS (April 18, 2025), https://www.irs.gov/irm/part11/irm_11-003-041#idm140113567748240.

A. Defendants Have Effectuated the Data Policy to Widely Share Taxpayer Data Throughout the Federal Government.

Defendants have directed adoption of the new IRS Data Policy that abandoned the agency's prior promise that taxpayer information be kept confidential, including within the government, and that access and disclosures be strictly minimized.[18] The Data Policy (1) greatly expands access to and use of taxpayer information within the IRS; (2) consolidates data systems to facilitate broad, not segregated access within the agency; and (3) permits large-scale data-sharing with other agencies, unrelated to tax administration.[19]

Although the IRS has not announced the Policy publicly, it is apparent from recent IRS actions. For example, DOGE Affiliates at the IRS are building a single, unified database of taxpayer information within the IRS including through the use of a software tool—known as an application programming interface ("API")—that will permit automated access to all IRS taxpayer information by IRS employees in one interface.[20]

The new Data Policy is also revealed by, and led to significant changes in, how the IRS shares taxpayer information with other federal agencies for non-tax purposes. IRS DOGE Affiliates have worked to create an "omnibus" agreement, to allow federal agencies broad access to taxpayer information.[21] The IRS also finalized a broad agreement to share IRS data with ICE. *See* Ex. 4. Reflective of the policy, a whistleblower disclosed to Congress in April that DOGE

---

[18] *See* Makena Kelly, *Palantir Is Helping DOGE With a Massive IRS Data Project*, WIRED (Apr. 11, 2025), https://perma.cc/AF3S-6QP7.
[19] *Id.*; Ex. 4; Ex. 1.
[20] Makena Kelly, *DOGE Is Planning a Hackathon at the IRS. It Wants Easier Access to Taxpayer Data*, WIRED (Apr. 5, 2025), https://perma.cc/3LRJ-FUAX; Rebecca Heilweil, *DOGE Rep Sam Corcos is Treasury's New Chief Information Officer, Source Says*, FedScoop (May 6, 2025), https://perma.cc/R34N-D8SB.
[21] Jacob Bogage & Jeff Stein, *DOGE Presses to Check Federal Benefits Payments Against IRS Tax Records*, Wash. Post (Mar. 1, 2025), https://perma.cc/EDZ5-53FK.

was building a "massive database of SSA data and data from across the federal government, including the [IRS], Department of Health and Human Services (HHS), and other agencies" and doing so "in a manner that disregards important cybersecurity and privacy considerations, potentially in violation of the law."[22] The Administration also intends to cross-reference and "reconcile" databases at different agencies for the purpose of "eliminat[ing] the waste and fraud,"[23] and, also has moved to gather information on SNAP recipients into a federal database that can be cross-referenced with other data,[24] like IRS taxpayer data.[25]

Some members of senior leadership at the IRS have resisted the new Data Policy, including on the basis that it violates the law, and have then been pushed out of the agency.[26] These leaders include multiple Acting IRS Commissioners, the Chief Risk Officer, the Chief Privacy Officer, the Chief Financial Officer, the Chief Information Officer, the subsequent Chief Information Officer, and approximately 50 senior IRS IT executives.[27]

---

[22] H. Comm. on Oversight & Gov't Reform Democrats, Press Release, *Disturbing Whistleblower Information Obtained by Committee Democrats Leads Ranking Member Connolly to Demand Investigation into DOGE's Disruption of Social Security Operations, Collection of Americans' Sensitive Data* (Apr. 17, 2025), https://perma.cc/24PE-7T6Z.

[23] Coral Davenport, *DOGE Accesses Federal Payroll System Over Objections of Career Staff*, N.Y. Times (Mar. 31, 2025), https://perma.cc/L6L3-7REC.

[24] 90 Fed. Reg. 26521 (June 23, 2025).

[25] Jude Joffe-Block & Stephen Fowler, *USDA, DOGE demand states hand over personal data about food stamp recipients*, NPR (May 9, 2025), https://perma.cc/5LJP-2SZH.

[26] Nathan Layne & Kanishka Singh, *Top IRS Officials Join Chief in Quitting Following Immigration Data Deal*, Reuters (Apr. 9, 2025), https://perma.cc/X3JX-G5ZF; Erin Slowey, *IRS Head, Privacy Chief to Quit After Immigration Data Deal (1)*, Bloomberg Tax (Apr. 8, 2025), https://perma.cc/HMF6-FYLL; Matt Bracken, *IRS Cuts About 50 IT Executives, Sources Say*, FedScoop (Mar. 29, 2025), https://perma.cc/J8DT-MGYW.

[27] *See also* Natanson, *et al.*, *DOGE aims to pool federal data, putting personal information at risk*, Wash. Post (May 7, 2025), https://perma.cc/9JCK-9K4W/ (losing even "three agency leaders in three months is 'unprecedented'").

B. Defendants Are Now Implementing the Data Policy at Scale, Responding to Mass ICE Requests for IRS Data.

Defendants are now implementing the Data Policy, sharing sensitive taxpayer data at enormous scale. The IRS has acknowledged that information sharing with ICE has begun and that is being carried out pursuant to the Memorandum of Understanding ("MOU") it executed with ICE in April 2025 and pursuant to Section 6103(i)(2).[28] The MOU authorizes ICE to request "address information," specifically "the last known address for each individual in each request." *See* Ex. 4, at 2. The MOU incorporates the requirements in Section 6103(i)(2) of the Internal Revenue Code and requires ICE to provide in its request the taxpayer's name and address, the relevant tax year, the criminal statutory provision under which the taxpayer is facing an investigation, and the identity of "the ICE officers and employees personally and directly engaged in the nontax criminal investigation." *See* Ex. 4, at 3. Given that the stated purpose of the MOU is to obtain accurate, current addresses, the "address" that it says ICE will include in requests is presumably one known to be out of date or inaccurate. The agreement also restates the Section 6103(i)(2) requirement that information is only to be used "by officers and employees of ICE solely for the preparation for judicial or administrative proceedings, or investigation that may lead to such proceedings" under the criminal statute specified in their request. *Id.*

Despite the statutory and MOU requirements that limit the IRS to sharing data only when specific requirements met, including identification of law enforcement officers "personally and directly engaged" in the relevant criminal investigation, the scale of recent data sharing is massive and rapid. In the week of August 4, 2025, ICE requested that the IRS provide the personal information for 1.23 *million* individuals in a mass request for data on individuals that

[28] Defs.' Notice in Status of Requests for Return Information, *Centro de Trabajadores Unidos v. Bessent*, No. 1:25-cv-00677 (D.D.C. Aug. 12, 2025), ECF No. 72 (Ex. 5).

ICE believes are in the country without valid immigration status. *See* Ex. 1. The IRS processed this request within days and provided home addresses from the tax return information of tens of thousands of individuals before the end of the week, *id*., despite statutory bars and long-standing policies against such disclosures. White House officials pushed the IRS to release even more information, including whether the individuals the IRS identified had claimed the Earned Income Tax Credit.[29] Shortly after the IRS refused that request, the President removed the recently confirmed IRS Commissioner and replaced him with Defendant Treasury Secretary Bessent in an acting capacity.

This mass sharing of data under the Data Policy follows the then-acting general counsel of the IRS Andew De Mello's refusal "to turn over the addresses of 7.3 million taxpayers sought by ICE" after identifying numerous legal deficiencies in the agency's request.[30] Two days later, he was forced out of his job.[31] Another former senior IRS official stated that demands for this amount of data, for these purposes, was "unprecedented" and amounted to "a big data dump."[32] This request was also under the MOU between the IRS and ICE.[33]

The disclosures now occurring from the IRS to ICE within a single week under the Data Policy are unprecedented. In 2023, the IRS reported no disclosures to DHS. In total the agency reported 75,647 disclosures to the Department of Justice, U.S. Attorneys, and other federal law

[29] Jacob Bogage & Kadia Goba, *IRS, White House clashed over immigrants' data before tax chief was ousted*, Wash. Post (Aug. 9, 2025), https://perma.cc/K2PN-WEKR (Ex. 2).
[30] William Turton, *et al.*, *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, ProPublica (July 15, 2025), https://perma.cc/6XGQ-KX6T (Ex. 3).
[31] *Id*.
[32] *Id*.
[33] Aravind Vodupalli, *The New ICE-IRS Data Sharing Agreement Has Three Problems*, Tax Pol'y Ctr. (Apr. 21, 2025), https://perma.cc/FY7J-VTL8 (citing Ex. 4).

enforcement agencies.[34] The year before, it reported 43,141 disclosures to those agencies, and none to DHS.[35] The recent disclosures made in a matter of days rival the total annual IRS disclosures under 6103(i)(2) to *all* law enforcement agencies, and the IRS has never made such disclosures to ICE.

The IRS has represented in court that "IRS cannot share information under Section 6103(i)(2) for civil immigration enforcement."[36] However, the Administration has clearly stated that the purpose of the IRS's data sharing *is* to support civil enforcement of immigration laws,[37] rather than to conduct *bona fide* investigations of non-tax criminal laws. In response to investigative reporting by ProPublica in July 2025, detailing the mechanics of the IRS's data sharing process with ICE, a White House spokesperson said:

> ProPublica . . . suggests we should turn a blind eye to criminal illegal aliens present in the United States for the sake of trying to collect tax payments from them. . . . This isn't a surveillance system. . . . It's part of President Trump's promise to carry out the mass deportation of criminal illegal aliens. . . ."

See Ex. 3.

III. The Implementation of the Data Policy Harms Plaintiffs, Their Clients, and Their Members.

The impact of the IRS's effectuation and implementation of the Data Policy through its mass data sharing with ICE has been swift and significant, including harms to (1) the Center's

---

[34] IRS, Joint Comm. on Tax'n, *Disclosure Report For Public Inspection Pursuant To Internal Revenue Code Section 6103(P)(3)(C) For Calendar Year 2023 (JCX-14-24)* (Apr. 25, 2025), https://perma.cc/5A86-ZSJN.

[35] IRS, Joint Comm. on Tax'n, *Disclosure Report For Public Inspection Pursuant To Internal Revenue Code Section 6103(p)(3)(C) For Calendar Year 2022 (JCX-6-23)* (Apr. 18, 2023), https://perma.cc/GM8S-R5KU.

[36] Defs.' Resp. to Amicus Brs., *Centro de Trabajadores v. Bessent*, Case No. 25-677-DLF (D.D.C. May 7, 2025), ECF No. 66.

[37] A deportation (i.e., removal) proceeding is a "a purely civil action." *I.N.S. v. Lopez-Mendoza*, 468 U.S. 1032, 1038 (1984).

clients and Plaintiffs' taxpaying members, whose data has already been disclosed or is at imminent risk of disclosure for purposes of immigration enforcement and in violation of the law and their privacy interests, (2) the Center's ability to provide services, advise its clients, and further its mission, and (3) the Center's clients and MSA's members' ability to interact with the tax system to receive benefits to which they are entitled.

The IRS has, to date, disclosed to ICE the confidential information of tens of thousands of taxpayers. Immigrant taxpayers, including the Center's clients and MSA's members, have either been included in these disclosures or face an imminent risk that their data will be disclosed. ICE has asked IRS to provide data about as many as 7.3 million taxpayers, *see* Ex. 3—a number that likely exceeds the total number of active ITIN holders, *see* Declaration of Nina Olson, Ex. 6 ("Olson Decl.") ¶ 74, suggesting all ITIN holders will likely be swept up in this data transfer. ITIN tax filers number among the Center's clients and MSA's members. Olson Decl. ¶ 17, 42; Declaration of Shawn Phetteplace, Ex. 7 ("Phetteplace Decl.") at ¶ 9.

Immigrant taxpayers whose data is disclosed are also placed at heightened risk of having that data used illegally for immigration enforcement, exposing them to ICE raids, detention, and even removal from the country. Given the risks of misidentification posed by this process, *see* Olson Decl. ¶ 75-78; Phetteplace Decl. ¶ 15; Declaration of Jane Doe, Ex. 8 ("Jane Doe Decl.") ¶ 23-24, all taxpayers whose data is shared face this risk, regardless of whether they have pending orders of removal or are otherwise subject to immigration enforcement. The IRS's data-sharing practices have consequently instilled deep and legitimate fear in immigrant communities. *See* Olson Decl. ¶ 50, 62-63, 72-75; Phetteplace Decl. ¶ 7-8, 12-14. And these risks, caused by the IRS's data-sharing, are standing in the way of people—including the Center's clients and MSA's members, on whose behalf they sued—engaging with the tax system by applying for

ITINs, filing tax returns, or otherwise engaging in IRS processes, losing time-sensitive opportunities to preserve their rights, including to benefits to which they are entitled. *See* Olson Decl. ¶ 79-90); Phetteplace Decl. ¶ 14. For example, at least one of the Center's Low Income Taxpayer Clinic ("LITC") clients is choosing to forgo a $500 credit to which they are entitled, to avoid providing further information to the IRS in fear of its being shared (Olson Decl. ¶ 48); at least one client is entitled to a refund of excess tax withholdings, but is electing not to file a tax return for the same reason (*Id*. ¶ 49). In these and other cases, the pecuniary losses will become irrevocable if the taxpayer cannot safely file a return by the relevant IRS deadline. (*Id*. ¶ 89)

Members of Plaintiff MSA—including small business owners who are immigrants and who employ immigrants and ITIN filers (Phetteplace Decl. ¶ 6; Jane Doe Decl. ¶ 26), as well as include low-income sole proprietors eligible for the EITC, CTC, and other refundable credits (MSA Decl. ¶ 4, 12; Jane Doe Decl., ¶ 10, 23), face similar harms in connection with their personal and business-related tax returns. Some MSA members are themselves or have spouses or family members in the category of taxpayers targeted for this unlawful data sharing. Phetteplace Decl. ¶ 8. Others face challenges to their businesses because their employees are harmed. Phetteplace Decl. ¶ 6, 8, 10; Jane Doe Decl. ¶ 26-28.

The Center itself is also suffering organizational harm from Defendants' actions. It faces significant hurdles to fulfil its mission and to provide the services and programming on which its clients, members, and communities rely. Its mission is to advance taxpayer rights, promote trust in the tax system, and increase access to justice in the tax system. Olson Decl. ¶ 3-6. Its work focuses on the most vulnerable populations, including immigrants, people whose first language is not English, low-income people, and domestic violence survivors. *Id*. ¶ 3. Plaintiffs pursue this mission by, *e.g.*: (1) running a LITC, *id*. ¶ 4, 7-18; (2) conducting education and outreach on the

role taxpayer rights play in promoting "trust in systems of taxation," *id*. ¶ 6, 21-27; and (3) running LITC Connect, a nationwide network of other LITCs, attorneys, accounts, and enrolled agents, id. ¶ 19-20. The trust and confidentiality protections afforded by the law—and, historically, by the IRS—are foundational to the Center's work, and the Center relies upon them. *Id*. ¶ 28-39. Since its founding, the Center has advised and encouraged its clients and target populations to file their taxes, because their information is adequately protected by the IRS and will not be used for immigration enforcement purposes. *Id*. ¶ 34, 47. The Data Policy has made that almost impossible, despite dedication of more time, money, and resources to these efforts.

Because of the IRS's data sharing with ICE, taxpayers and prospective taxpayers "have become less willing to come to the Center's events, seek its guidance, or engage with the Center's education and outreach," and—for example—the Center has held only a tenth of the events it did compared to last year. *Id*. ¶ 41-44. These obstacles materially limit the Center's ability to further its mission of promoting trust in the tax system or its funding-related obligations to educate these taxpayer populations about their rights and responsibilities. *Id*. ¶ 40-46. Although the Center has dedicated increased resources to these efforts, it still faces a significant frustration of its mission. *Id*. ¶ 45-46, 52-53. Once these taxpayers' trust in the tax system is lost, it will be very difficult—and, for some taxpayers, impossible—to restore. *Id*. ¶ 53.

The Data Policy has also created significant obstacles to the Center serving its clients. Id. ¶ 47-51. The Center's LITC can also no longer responsibly provide substantive advice to its immigrant clients about whether they can safely—or should—engage with the IRS by applying for ITINs, filing tax returns, or otherwise participating in IRS processes. *Id*. ¶ 47. Although the law provides strong privacy protections, the Center's attorneys cannot reconcile the IRS's current conduct with the law. *Id*.

LITC Connect members are suffering similar harms. *Id*. ¶ 55-68. They "are also experiencing a significant drop-off in the willingness of taxpayers to attend and engage with their education and outreach efforts, particularly among those who do not speak English as a first language and who are more likely to be immigrants." *Id*. ¶ 55. The volume of calls from Hispanic taxpayers has noticeably decreased and is nearing a standstill. *Id*. ¶ 56. The Center's LITC Connect is designed to support these member clinics and practitioners. The Center is unable to navigate this drastic and unlawful change, and it has harmed its ability to provide advice, outreach, and support to the network. *Id*. ¶ 69-70.

The members of Plaintiffs National Federation of Federal Employees ("NFFE") and Communications Workers of America ("CWA") are also harmed by the Data Policy and its implementation to permit mass disclosures of sensitive taxpayer information to ICE. Plaintiff unions NFFE and CWA have hundreds of thousands of public and private sector members and employees whose sensitive information—including their Social Security or taxpayer identification numbers; names and addresses; taxable income; marital status; and information, such as medical expenses, relating to eligibility for tax deductions and credits—is held by the IRS. Am. Compl. ¶ 47–53; Declaration of Yvette Piacsek, Ex. 9 ("Piacsek Decl.) ¶ 3; Declaration of John Doe, Ex. 10 ("John Doe Decl.") ¶ 3-4. They each have members who are low-income workers eligible for the Earned Income Tax Credit ("EITC") and the Child Tax Credit ("CTC"). Am. Compl. ¶ 49–50, 53; Piacsek Decl. ¶ 5. Many NFFE members are citizens who immigrated to the United States and have family members and loved ones that they worry will be harmed by the Data Policy. Piacsek Decl. ¶ 6-9; John Doe Decl. ¶ 5-6.

LEGAL STANDARDS

The Administrative Procedure Act ("APA") permits plaintiffs to seek judicial review of "final agency action for which there is no other adequate remedy in a court." 5 U.S.C. § 704. Reviewable "agency action" "includes the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act." 5 U.S.C. § 551(13). A reviewing court shall "hold unlawful and set aside" agency actions found to be "arbitrary, capricious," or "otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

Section 705 of the APA authorizes a court to "issue all necessary and appropriate process to postpone the effective date of an agency action or to preserve status or rights pending conclusion of the review proceedings." 5 U.S.C. § 705. The court may do so "[o]n such conditions as may be required and to the extent necessary to prevent irreparable injury." *Id*. "The factors governing issuance of a section 705 stay are the same as those that govern the grant of a preliminary injunction." *Coal. for Humane Immigrant Rts. v. Noem*, No. 25-872-JMC, 2025 WL 2192986, at *12 (D.D.C. Aug. 1, 2025). To obtain this preliminary relief, "the moving party must show: (1) a substantial likelihood of success on the merits, (2) that it would suffer irreparable injury if the [preliminary relief motion] were not granted, (3) that [such an order] would not substantially injure other interested parties, and (4) that the public interest would be furthered" by the order. *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006). "In a case like this one, where the Government is the non-movant, the third and fourth factors merge." *Coal. for Humane Immigr. Rts.*, 2025 WL 2192986, at *12.

ARGUMENT

I. Plaintiffs are Likely to Succeed on the Merits of Their Claims Because the Data Policy Violates the APA.

A. The Data Policy is Final Agency Action and There Is No Adequate Remedy Other Than APA Review

The Data Policy—described above, *see, supra,* Background § II— (1) greatly expands access to and use of taxpayer information within the IRS; (2) consolidates data systems to facilitate broad, not segregated access within the agency; and (3) permits large-scale data-sharing with other agencies, unrelated to tax administration, amounts to a wholesale rewrite of the IRS's data privacy policy. The Data Policy constitutes final agency action and is subject to the APA's provisions for judicial review.

Final agency actions are those (1) which "mark the consummation of the agency's decisionmaking process," as opposed to decisions of a "merely tentative or interlocutory nature;" and (2) "by which rights or obligations have been determined, or from which legal consequences will flow." *Army Corps of Eng'rs v. Hawkes Co*, 578 U.S. 590, 597 (2016). Consummation means that the agency has reached a decision on the issue before it and effectuated it in some manner; it need not be reduced to a written statement. *See, e.g., Her Majesty the Queen*, 912 F.2d at 1531 ("[T]he absence of a formal statement of the agency's position, as here, is not dispositive[.]"); *R.I.L-R v. Johnson*, 80 F. Supp. 3d 164, 184 (D.D.C. 2015) ("Agency action . . . need not be in writing to be final and judicially reviewable.").

D.C. Circuit precedent leaves no doubt that a policy permitting disclosure of information is final agency action. In *Venetian Casino Resort v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008), the court of appeals held that the EEOC's adoption of a policy allowing disclosure of an employer's confidential information without notice to that employer constituted final agency

action reviewable under the APA. The D.C. Circuit viewed this as so self-evident that the sum of its discussion of the issue is that the policy "is surely a 'consummation of the agency's decisionmaking process,' and 'one by which . . . rights [and] obligations have been determined.'" *Id*. (quoting *Bennett*, 520 U.S. at 177–78); *see also Chrysler Corp. v. Brown*, 441 U.S. 281, 318-19 (1979) (holding that a "decision to disclose [reports under FOIA] is reviewable agency action" under the APA).

Defendants' action constitutes final agency action. In evaluating the first *Bennett* prong, the D.C. Circuit considers "whether the action is 'informal, or only the ruling of a subordinate official, or tentative.'" *Soundboard Ass'n v. F.T.C.*, 888 F.3d 1261, 1267 (D.C. Cir. 2018) (quoting *Abbott Labs v. Gardner*, 387 U.S. 136, 151 (1967)). The decision to disclose extraordinarily sensitive government information and data protected by law to other agencies, and to do so without a permissible purpose is not tentative or informal; rather, it is a final determination of agency policy and practice. Further, agency leadership approval of an agency action is a "signpost[] of authoritative determination, finality[,] and ripeness." *Nat'l Automatic Laundry & Cleaning Council v. Shultz*, 443 F.2d 689, 702 (D.C. Cir. 1971). As discussed *supra,* any leadership that has disagreed with the implementation of Defendants' new policy has been quickly removed from their position or pushed out of the IRS.

Defendants' action also recognizes that this action is not informal; the Data Policy has been implemented in several concrete ways, including through the data-sharing agreement with ICE that far exceeds what had previously been permissible under IRS policy and the development of the technical infrastructure necessary for mass data sharing. *See*, *supra*,

Background § II(A).[38] Now, Defendants have actually shared unprecedented swaths of taxpayers' data with ICE under this new Data Policy, establishing its finality. *See*, *supra*, Background § II(B). This action is not tentative; the policy has been implemented, and disclosure of sensitive information, pursuant to the Data Policy, has begun. Analysis of the second *Bennett* prong is equally clear: Defendants' decision has determined their obligations to disclose data and information within their control and the right of DOGE Affiliates, IRS employees, and other agencies to access it. It has also affected the rights of the individuals and entities with privacy interests in that data and created significant legal consequences via unlawfully expanding access to and disclosure of taxpayer information in violation of those individuals' statutory rights to have that data protected under the Internal Revenue Code. As in *Venetian Casino*, such actions determine rights and obligations. 530 F.3d at 931.

Further, there is no other adequate remedy available that would preclude the court's review of this action under the APA. In assessing whether such an alternative "adequate remedy" exists, there is a strong presumption that agency actions are reviewable under the APA. *Abbott Labs* 387 U.S. at 140. Here, the only other plausible remedies to the Data Policy are discrete damages provisions for unlawful access or disclosure under the Internal Revenue Code. *See* 26 U.S.C. § 7431. Backward-looking damages for discrete instances of unlawful access are inadequate to address a policy of ongoing data sharing at mass scale. Other courts in this circuit have repeatedly held that similar provisions within the Privacy Act do not provide an adequate remedy precluding APA review. The same logic applies here. *See Doe v. Stephens*, 851 F.2d 1457, 1460–61, 1463 (D.C. Cir. 1988); *Radack v. DOJ*, 402 F. Supp. 2d 99, 104 (D.D.C. 2005);

[38] As noted *supra* note 17, Defendants have also revised the IRS Manual to remove privacy safeguards and procedural barriers to effectuating the MOU.

AFL-CIO v. DOL, No. 25-339, 2025 WL 1129227, at *16 (D.D.C. Apr. 16, 2025) (citing *Doe v. Chao*, 540 U.S. 614, 619 n.1 (2004)). The Data Policy is reviewable final agency action.

B. The Data Policy Violates the Internal Revenue Code

Under the APA, a reviewing court shall "set aside agency action . . . found to be . . . not in accordance with law" or "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(A), (C). An "agency action is 'not in accordance with law' if it violates some extant federal statute or regulation." *Ovintiv USA, Inc. v. Haaland*, 665 F. Supp. 3d 59, 72 (D.D.C. 2023). The Data Policy is contrary to law because it authorizes widespread sharing of protected taxpayer data across the federal government, without necessary safeguards, that necessarily violates Section 6103. The Data Policy also exceeds statutory authority, as nothing permits the disclosures made and imminently planned by the IRS. *See* 5 U.S.C. § 706(2)(A), (C). The IRS's MOU with ICE and its recent sharing of return information *en masse*—both carried out under the Data Policy—demonstrate the Policy's unlawfulness because they violate the stringent requirements of Section 6103(i)(2).

Sec. 6103(i)—the only exception to the confidentiality of taxpayer information that the IRS or ICE has invoked in connection with these data transfers—permits disclosures to federal officers or employees for administration of federal laws not relating to tax administration. See 26 U.S.C. § 6103(i). Subpart (1) allows disclosures only pursuant to a court order. *Id*. at § 6103(i)(1). Subpart (2) allows for the disclosure of a narrower category of information—"return information other than taxpayer return information," for use in criminal investigations, without requiring a court order. *Id*. at § 6103(ii). The requesting agency must provide: (i) the *name and address* of the taxpayer with respect to whom the requested return information relates; (ii) the taxable period or periods to which such return information relates; (iii) the statutory

authority under which the proceeding or investigation is being conducted; and (iv) the *specific reason* or reasons why such disclosure is, or may be, relevant to such proceeding or investigation. *Id*. The limited category of information that may be disclosed under (i)(2) excludes any information provided to the IRS by or on behalf of the taxpayer themselves. *Id*. As the Internal Revenue Manual explains, 6103(i)(2) requests are typically made by U.S. Attorney's Offices requesting such things as "fact of filing information" (i.e. whether an individual has filed a tax return).[39]

Sec. 6103(i)(2) requires guardrails for disclosing this limited subset of return information, but the IRS's recent transfer of data to ICE breached them all. First, the IRS may only disclose data after receiving a request "which meets the requirements of subparagraph (B)." 26 U.S.C. § 6103(i)(2)(A). However, the IRS cannot have undertaken any meaningful review of the *en masse* request it received from ICE to ensure compliance, given the speed with which it was processed. Rather than requiring a careful review by IRS employees, the IRS developed an automated process that simply processes searches and returns results as long as ICE filled in all the columns in a spreadsheet. *See* Ex. 3. Thus, the IRS was able to process as many as 1.23 million requests for information, within days of receipt of the requests. *See* Ex. 1. In making these automated disclosures, the IRS cannot be complying with its obligations to confirm compliance with Section 6103(i)(2) before transferring data.

Second, Section 6103(i)(2) requires that the request include "the name and address of the taxpayer." Under the plain text of the statute, the requests fail to meet this requirement. Yet ICE is *seeking* addresses for these individuals. *See* Ex. 1. While DHS may have former or inaccurate

[39] IRM § 11.3.28.4, *Disclosure of Return Information (Other Than Taxpayer Return Information) Pursuant to IRC 6103(i)(2),* IRS (April 17, 2025), https://perma.cc/AN57-7XR8 at (4).

addresses, the statute is straightforward—it requires that the requester include the "name and address," not name and a *former* address, or a *suspected* address. There are good reasons for this requirement, including ensuring that the IRS provides information on the correct taxpayer in response to a request.

It is also why for over 40 years the IRS has interpreted the law to prohibit disclosures under Section 6103(i)(2) for requests seeking address information. This question has been assessed by numerous administrations. In 1982, the IRS determined addresses should not be disclosed under 6103(i)(2). *See* Olson Decl. ¶ 31; *Wayte v. United States*, 470 U.S. 598, 613 (1985) (noting that the Secret Service had attempted to obtain address information from the IRS, but could "gain no useful access" to the data under the 26 U.S.C. § 6013). This position has remained consistent since 1982.[40] Indeed, he IRS Manual is clear: "Requests for addresses only are invalid because IRC 6103(i)(2) requires that the requester provide an address."[41] The Court's "respect" is "especially warranted" for this "Executive Branch interpretation [that] was issued roughly contemporaneously with enactment of the statute and remained consistent over time." *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 386 (2024). The Data Policy is contrary to law.

Reading Section 6103(i)(2) in the "context of the statute as a whole" reinforces the conclusion that it does not permit sharing taxpayers' addresses to allow ICE to locate individuals for immigration enforcement or because of a suspicion of criminal conduct. *See Robinson v.*

---

[40] *E.g.*, GAO, *Internal Revenue Service: Individual Taxpayer Identification Numbers Can Be Improperly Obtained and Used* (Mar 10, 2004), https://perma.cc/AK35-2P6V ("Section 6103 ... allows IRS to disclose taxpayer information to federal agencies and authorized employees of those agencies, but only under specific conditions. Section 6103 does not currently authorize data sharing between IRS and DHS specifically for immigration enforcement.")

[41] IRM § 11.3.28.4, *supra* n.39, at (5); *see also* IRS Pub. 4639, *Disclosure & Privacy Law Reference Guide,* 5–4 (rev. 2012), https://perma.cc/3GQR-TPWT ("Requests under section 6103(i)(2) seeking only taxpayers' addresses do not comply with the section.")

Shell Oil Co., 519 U.S. 337, 341 (1997). There is a separate provision of 6103(i) designed for these purposes: 6103(i)(5) explicitly pertains to disclosures to "locate fugitives from justice." Statements by the Administration, as well as the MOU between ICE and the IRS, make clear that locating individuals suspected of violating immigration law, not prosecuting them criminally, is the intent of the disclosures at issue here. *See* Ex. 3; Ex. 4. But disclosures under 6103(i)(5), for "use in locating [an] individual," require a court order; Defendants do not have one.

Third, the IRS is authorized to provide the requested information *only* to specific officers and employees of the requesting agency who are "personally and directly engaged" in preparation for a criminal judicial or administrative proceeding, an investigation which may result in such a proceeding, or certain grand jury proceedings. 26 U.S.C. § 6103(i)(2). It does not permit the IRS to disclose information to a receiving agency liaison or data analyst, to be further passed along at the receiving agency's discretion. Rather, Section 6103(i)(2) specifies that the information may be used by *only* those officers and employees personally and directly engaged in that preparation, as identified in the request, and *solely* for that preparation. *Id*. This requirement is an important safeguard against broad dissemination of confidential information, after it leaves the IRS's control. ICE—an agency of around 21,000 employees, across all functions[42]—cannot have identified enough employees to competently attest they are "personally and directly engaged" in criminal investigations of 1.23 million people, or even 40,000.

Fourth, whether a taxpayer qualifies for the Earned Income Tax Credit ("EITC") is "taxpayer return information" and cannot be disclosed in response to a Section 6103(i)(2) request. Yet when the White House contacted the IRS on August 8 to follow up on ICE's

[42]DHS, U.S. Immigration and Customs Enforcement, Budget Overview (Fiscal Year 2024), https://perma.cc/F23X-EU4J, at 7.

requests, officials requested additional information on the taxpayers the IRS identified—specifically, whether any had claimed the EITC. *See* Ex. 1; Ex. 2. This too violated the statute.[43]

Fifth, taxpayer information may only be disclosed based on—and must be used *solely* for purposes of preparation for—a criminal judicial or administrative proceeding, an investigation which may result in such a proceeding, or certain grand jury proceedings. 26 U.S.C. § 6103(i)(2). While the information ICE seeks here may *relate* to individuals facing deportation and who could theoretically be subject to federal criminal investigation, it is *sought* to confirm their home addresses so they can be located. *See* Ex. 1. And exclusion and removal of non-citizens in the United States is a matter of *civil* immigration law, not federal criminal law. ICE intends to use the information for removal or deportation purposes, as the Administration has stated both publicly and in the MOU; [44] the disclosures are therefore unlawful.

This requirement is set forth twice in (i)(2). It states that recipients of the information may only use the information for the preparation for a proceeding or an investigation that may result in such a proceeding, and that any requests for disclosure must set forth the "*specific* reason or reasons why such a disclosure is, or may be, relevant to such proceeding or investigation." *Id*. ICE's requests for information on tens or hundreds of thousands of taxpayers cannot set forth a *specific* reason for each disclosure. A boilerplate reason for all individuals

[43] The White House, incidentally, is not entitled to request taxpayer information from the IRS under Section 6103(i)(2); it may only do so under a different provision—Section 6103(g)—and there is no indication that such a request was properly made here.

[44] The MOU Introduction (Ex. 4, p. 1) emphasizes the impetus for the agreement as Exec. Order No. 14161, which directs certain agencies to "take immediate steps to identify, exclude, or remove aliens illegally present in the United States." Exec. Order No. 14161, *Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats*, 90 Fed Reg. 8451 (Jan. 30, 2025). *See also* Ex. 3 ("It's part of President Trump's promise to carry out the mass deportation of criminal illegal aliens.")

would not be "specific," or that word would have no meaning in the statute. These disclosures under the Data Policy are therefore also violative of Section 6103(i)(2).

That the IRS did not locate matches for and disclose data about all of the people identified in ICE's request provides Plaintiffs with little relief; the IRS disclosed information about tens of thousands of taxpayers already, and the same day that the IRS said it could not satisfy the balance of the request, Commissioner Long was "ousted" by the Administration. *See* Ex. 2. Such an act makes clear: wide disclosure of data under the Data Policy is required, and anyone who opposes or expresses concerns with its legality and implementation, particularly with respect to disclosures to DHS, will be removed.

Courts must exercise their "independent judgment in deciding whether an agency has acted within its statutory authority." *Loper Bright*. In this instance, Defendants have not. Thus, the Data Policy is unlawful and must be stayed with respect to these disclosures to ICE.

C. The Data Policy is Arbitrary and Capricious

Defendants' Data Policy is also arbitrary and capricious. The APA "requires agencies to engage in "reasoned decisionmaking." *DHS v. Regents of the Univ. of Cal*., 591 U.S. 1, 16 (2020) (quoting *Michigan v. EPA*, 576 U.S. 743, 750 (2015)). That requires the agency to "articulate a satisfactory explanation for its action," which includes "display[ing] awareness that it is changing position" and "that there are good reasons for the new policy." *FCC v. Fox Tele. Stations, Inc.*, 556 U.S. 502, 513, 515 (2009). Agency actions "must examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made." *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (internal quotation marks and citation omitted). "Normally, an agency [action] would be arbitrary and capricious if the agency . . . entirely failed to consider an

important aspect of the problem . . . or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise." *Id.* And finally, an agency must provide "a more detailed justification than what would suffice for a new policy created on a blank slate" when "its prior policy has engendered serious reliance interests that must be taken into account." *Id*. at 515; *see also Am. Bar Ass'n v. Dep't of Educ*., 370 F. Supp. 3d 1, 33 (D.D.C. 2019).

1. The Defendant Agencies Have Not Acknowledged or Justified Their Change in Policy

Defendants' Data Policy has led to the disclosure of sensitive data regarding thousands of individuals, with potentially tens of thousands to millions more imminent, with no meaningful acknowledgement or justification from the Defendants regarding this significant change in position. "[A]n '[u]nexplained inconsistency' in agency policy is 'a reason for holding an interpretation to be an arbitrary and capricious change from agency practice.'" *Encino Motorcars v. Navarro*, 579 U.S. 211, 222 (2016). "An agency may not . . . depart from a prior policy *sub silentio* or simply disregard rules that are still on the books," and it must "show that there are good reasons for the new policy." *State Farm*, 556 U.S. at 515. While an agency need not "demonstrate . . . that the reasons for the new policy are *better* than the reasons for the old one" or "provide a more detailed justification than what would suffice for a new policy created on a blank slate," it must at least "display awareness that it *is* changing position." *Id.*

In 2017, the IRS in the first Trump Administration made clear that it "has strong processes in place to protect the confidentiality of taxpayer information, and this includes information related to tax returns filed using ITINs."[45] The agency was clear that "[t]here is no

[45] Maria Sacchetti, *Undocumented and paying taxes, they seek a foothold in the American Dream*, Wash. Post (Mar. 11, 2017), https://perma.cc/8JVS-K4KR.

authorization under this provision to share tax data with ICE."[46] That position did not change during the following administration. "Requests for addresses only are invalid" under Section(i)(2) according to the IRS Manual.[47] But the recent mass disclosures of data from IRS to ICE, as well as the imminent additional disclosures, make plain: this policy has been reversed, without explanation. The Data Policy is unacknowledged and unexplained.

Defendants have failed to even attempt to present a reasoned basis for the wholesale changes they have made.[48] The Data Policy is, therefore, arbitrary and capricious. *E.g., Fox*, 556 U.S. at 513; *Encino Motorcars*, 579 U.S. at 222.

2. Defendants Failed to Consider Key Issues in Adopting the Data Policy

An agency action is arbitrary and capricious if the agency "failed to consider an important aspect of the problem." *Motor Vehicle Mfrs. Ass'n,* 463 U.S. at 43. In the scramble to consolidate internal access to and share with other agencies sensitive taxpayer information, Defendants lost sight of all other considerations—(1) the need to protect taxpayers' privacy, (2) the impact on participation and trust in the tax system, and (3) the harm that could result from disclosures, and in particular mistaken disclosures. Because Defendants did not consider these important factors, the policy is arbitrary and capricious.

First, the Internal Revenue Code and IRS's own regulations make clear it was important to consider taxpayers' privacy. The Taxpayer Bill of Rights gives individuals the right to privacy and the right to confidentiality. 26 U.S.C. § 7803(a)(3). Section 6103 makes clear that "returns and return information shall be confidential," with limited exceptions, and imposes criminal

[46] *Id*.
[47] IRM § 11.3.28.4, *supra* n.39, at (5).
[48] Defendants have not acknowledged or explained, for example, the changes it has made to the IRS Manual, *supra* note 17.

penalties for violations. IRS websites tell taxpayers that their information will be protected, and any examination by the IRS will be "no more intrusive than necessary."[49] Taxpayer data "is among the most confidential in the federal government."[50] Ex. 3; *see also* Koskinen Decl. ¶ 4-7. And rightfully so—the IRS holds incredibly sensitive information on millions of individuals and businesses.[51] Yet Defendants have provided no explanation to indicate they considered this critical factor.

Second, Defendants failed to evaluate the impact of the Data Policy, and the disclosures to ICE pursuant to it, on participation and trust in the tax system and, consequently, on tax revenue, which the Supreme Court has described as "the lifeblood of government." *Bull v. United States*, 295 U.S. 247, 259 (1935). Since 1985, the Internal Revenue Code has taxed "resident aliens"—including anyone who satisfies the "substantial presence" test defined in 26 U.S.C. § 7701(b)(3), regardless of immigration status—along with U.S. citizens, consciously sweeping in more taxpayers than have documented immigration status. Olson Decl. ¶ 14. And the IRS has "long assessed that it is critical to assure taxpayers that their sensitive information is protected and secure to support the integrity of the tax system and to encourage taxpayers to file returns and pay their taxes." Koskinen Decl. ¶ 7. For one, undocumented immigrants contribute significant revenue to the federal tax system—$59.4 billion in 2022 alone.[52] The IRS is expected to lose $12 billion in revenue this year, and more than $313 billion over the next decade, "as

[49] IRS, *Taxpayer Privacy Isn't Just a Right – It's the Law*, https://perma.cc/EP3T-HKRL (last visited Aug. 18, 2025).
[50] William Turton, *et al.*, *The IRS is Building a Vast System to Share Millions of Taxpayers' Data with ICE*, ProPublica (July 15, 2025), https://perma.cc/F87T-GUHB; *see also* Koskinen Decl.
[51] *See*, *e.g.*, Kris Cox, *IRS-ICE Agreement Weakening Privacy Protections Poses Risks for All* Taxpayers, Ctr. on Budget & Pol'y Priorities (Apr. 21, 2025), https://perma.cc/9D7T-MPXK.
[52] Carl Davis, et al., *Tax Payments by Undocumented Immigrants*, Inst. on Tax'n & Econ. Pol'y (July, 30, 2024), https://perma.cc/HV9A-TLAK; *see also* Liana Wang, *The IRS-ICE Deal Threatens All Workers*, OnLabor (May 26, 2025), https://perma.cc/CK3M-CG5U.

undocumented workers are poised to pay fewer taxes after the agency struck a deal to share data with U.S. immigration authorities."[53]

Further, trust and participation in the tax system facilitates the public benefit of individuals getting access to tax credits and refunds that Congress has determined they should have as a matter of public policy.[54] These include credits and deductions Congress has enacted to benefit people with children, with low incomes, paying for college, and others.[55]

Third, Defendants failed to consider the harm that could result from large-scale disclosures of taxpayer information under the Data Policy. Koskinen Decl ¶ 7 ("the confidentiality and limited sharing of taxpayer data is critical to preventing tax filing fraud by criminal actors using taxpayer information"). In particular, Defendants' automated haste under the Data Policy can reasonably be expected to "ramp up the risk of exposing data to hackers and other adversaries."[56] Searches run on name and (potentially out-of-date) address alone, as ICE seeks under the Data Policy, are likely to result in false positives and disclosure of the wrong individual's information to ICE. Olson Decl. ¶ 75-78. Tax and privacy experts reasonably "worry about how such a powerful yet crude platform could make dangerous mistakes":

---

[53] Augusta Saraiva, *IRS to Lose Billions in Revenue if Migrants Stop Filing Taxes*, Fortune (Apr. 9, 2025), https://perma.cc/Y6QV-7NQF; *see also* Julian Aguilar, *Tax-sharing Agreement Between ICE, IRS Could Cost Texas Billions in Tax Revenue, Experts Warn,* Houston Chronicle (Aug. 6, 2025), https://perma.cc/K5B9-P7WB.

[54] *See, e.g.*, Conor F. Boyle, et al., Cong. Rsch. Serv., R43805, The Earned Income Tax Credit (EITC): How It Works and Who Receives It (2023), https://perma.cc/T4TZ-DPSN; Nathan Anderson, *et al.*, *Why Are Millions of Dollars in Tax Refunds Going Unclaimed*, No. 1 ProfitWise News & Views (Mar. 2022), https://perma.cc/LF6W-F3GM.

[55] Cong. Rsch. Serv., R44825, The Earned Income Tax Credit (EITC): A Brief Legislative History (Apr. 26, 2017), https://perma.cc/9QV6-QCYL (The EITC "is now one of the federal government's largest antipoverty programs.")

[56] Hannah Natanson, *et al.*, *DOGE Aims to Pool Federal Data, Putting Personal Information at Risk*, Wash. Post (May 7, 2025), https://perma.cc/9JCK-9K4W.

> Because the search starts with a name instead of a taxpayer identification number, it risks returning the address of an innocent person with the same name as or a similar address to that of one of ICE's targets. The proposed system assumes the data provided by DHS is accurate and that each targeted individual is the subject of a valid criminal investigation. In effect, the IRS has no way to independently check the bases of these requests.

Ex. 3. Plaintiffs and their members fear that their taxpayer information will become wrapped up in this hasty, inaccurate process. Piacsek Decl. ¶ 9 (members "fear that the IRS's mass sharing of data with ICE will subject them to mistaken immigration enforcement actions based on misidentification"); Jane Doe Decl. ¶ 14 ("I have been a victim of identity theft in the past and therefore know all too well what it is like to have my information disclosed to someone else").

Defendants failed to consider any of these important issues prior to effectuating the Data Policy and disclosing data on a mass scale. Their decision to rush disclosure of sensitive data, without the normal guardrails that have long applied, was not "the product of reasoned decisionmaking." *See Motor Vehicle Mfrs. Ass'n*, 463 U.S. at 52.

3. The Data Policy Failed to Consider Reliance Interests

Defendants failed to account for the significant reliance interests of people who submit personally identifying information to the federal government on the understanding that such information shall be confidential and protected from disclosure, as articulated in the numerous declarations submitted in support of this filing. Piacsek Decl. ¶ 3; Phetteplace Decl. ¶ 16 ("For decades, MSA small business owners and their leaders have relied on reassurances by public officials, and the Tax Code itself to protect their sensitive information"); Jane Doe Decl. ¶ 13; Olson Decl. ¶ 32 ("These protections have been a cornerstone of the Center's ability to (1) effectively counsel our clients, and (2) provide education and outreach that encourages participation in the tax system").

The Data Policy also failed to consider immigrant taxpayers' reliance on prior public statements by the IRS and its officials that the agency "has no authorization under [the relevant] provision to share tax data with ICE."[57] *See also* Koskien Decl, ¶ 11 ("The IRS has historically… not shared taxpayers' information with immigration authorities for the purpose of locating individuals suspected to be present in the country illegally"). This has engendered significant reliance from immigrants, including MSA members and the Center's clients. MSA Decl. ¶ 6 ("MSA small business members include many immigrant-owned businesses. These, and other MSA small business members employ significant numbers of immigrants. They have trusted in the assurances of the IRS that their data would be kept confidential"); Olson Decl. ¶ 33 ("For example, we have, for years, assured our clients who are worried about confidentiality of the stringent protection in place at the IRS with respect to the protection of information").

The Center has also relied on these protections regarding the tax information of immigrants in offering services and programming to advance its mission. Olson Decl ¶ 35 ("We have, for example, encouraged undocumented immigrants to file for an Individual Tax Identification Number (ITIN) in order to participate in our tax system"). None of these interests were considered when Defendants began sharing significant amounts of sensitive data pursuant to the Data Policy. "When an agency changes course, as [Defendants] did here, it must be cognizant that longstanding policies may have engendered serious reliance interests that must be taken into account." *Regents of the Univ. of Cal.*, 591 U.S. at 30 (internal quotation marks and citations omitted). Because Defendants were not, the Data Policy is arbitrary and capricious and thus unlawful under the APA.

[57] Maria Sacchetti, *Undocumented and paying taxes, they seek a foothold in the American Dream*, Wash. Post (Mar. 11, 2017), https://perma.cc/X4ZL-2CMT.

II. Plaintiffs Face Irreparable Injury from the Continued Effect of the IRS Data Policy

Plaintiffs and their clients and members face irreparable harm if the Court does not act to stay the Data Policy pending resolution of this case. "An irreparable harm is an imminent injury that is both great and certain to occur, and for which legal remedies are inadequate." *Beattie v. Barnhart*, 663 F. Supp. 2d 5, 9 (D.D.C. 2009). Here, the harms suffered by both organizational Plaintiffs CTR and MSA and their clients and members satisfy this standard.

A. The Center Faces Irreparable Harm to its Organizational Interests

The D.C. Circuit has held that "organizational plaintiffs establish irreparable harm where defendants' actions 'perceptibly impair[] the organization's programs' and 'directly conflict with the organization's mission.'" *Cath. Legal Immigr. Network, Inc. v. Exec. Off. for Immigr. Rev.*, No. 21-00094, 2021 WL 3609986, at *3 (D.D.C. Apr. 4, 2021) (cleaned up); *see also Nat'l Treasury Emps. Union v. United States*, 101 F.3d 1423, 1430 (D.C. Cir. 1996) (looking to whether "a defendant's conduct has made the organization's activities more difficult" or "conflict[s] with the organization's mission"); *League of Women Voters of United States v. Newby*, 838 F.3d 1, 8 (D.C. Cir. 2016) (accord). Plaintiff CTR satisfies this test, which is sufficient to establish both irreparable injury to support entry of a preliminary injunction and standing. *See League of Women Voters*, 838 F.3d at 9 (holding that frustration of organization's mission demonstrates injury for purposes of both standing and irreparable harm).[58]

CTR faces irreparable harm to its ability to conduct effective education and outreach programs, its ability to counsel its LITC clients, and its facilitation of the LITC Connect network of LITCs, in direct conflict with and obstructing its ability to achieve its mission of promoting

[58] The Center also asserts third-party standing in this case to assert the interests of its clients. *See* Plaintiffs' Mem. in Opp'n to Defs' Mot. to Dismiss, ECF No. 27 (August 1, 2025), at 30-32.

trust in the tax system and advancing taxpayer rights. Each of these three categories of services and programs are "perceptibly impaired" by the Data Policy, which directly conflicts with CTR's mission. *Fair Emp. Council of Greater Wash., Inc. v. BMC Mktg. Corp.*, 28 F.3d 1268, 1276 (D.C. Cir. 1994) (quoting *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 379 (1982)).

"As the D.C. Circuit has confirmed, '[o]bstacles' that 'unquestionably make it more difficult for [an organization] to accomplish [its] primary mission ... provide injury for purposes both of standing and irreparable harm.'" *Vote Forward v. DeJoy*, 490 F. Supp. 3d 110, 130–31 (D.D.C. 2020) (quoting *Whitman-Walker Clinic, Inc.*, 2020 WL 5232076, at *38 (alterations in original) (quoting *League of Women Voters*, 838 F.3d at 9). Where an organization can explain "how the agency action 'forced it to divert or modify its activities in any meaningful way from its standard programmatic efforts,'" it can show a diversion of resources in support of a showing of irreparable harm. *Nat'l Ass'n for Advancement of Colored People v. United States Postal Serv.*, 496 F. Supp. 3d 1, 11–12 (D.D.C. 2020) (quoting *Int'l Acad. Of Oral Med. & Toxicology v. FDA*, 195 F. Supp. 3d 243 (D.D.C. 2016)).

Such is the case here. Particularly for the populations the Center serves, the Data Policy and current and ongoing transfers of home address information to ICE have significantly eroded trust in the tax system and made it materially more difficult for the Center to pursue its mission. Because of Defendants' conduct, these taxpayers can no longer rely on the confidentiality protections that have been in place for decades. Olson Decl. ¶ 39, 47. And the Center cannot accomplish its mission if taxpayers cannot safely engage in the tax system. When taxpayers are fearful and unwilling to engage, they do not attend the Center's education and outreach events, and the Center has already seen a significant drop-off in attendance, forcing the Center to devote and divert more resources to these efforts to fulfil its mission. *Id.* ¶ 41-46. These taxpayers

include ESL taxpayers who speak English as a second language ("ESL taxpayers"), to whom the Center is required to conduct specialized outreach as a condition of funding for its LITC. *Id.* ¶ 41. These taxpayers are also less willing to retain the LITC and engage with IRS processes, including to preserve their rights and obtain benefits to which they are entitled *Id.* ¶ 42, thereby frustrating the Center's delivery of client services and pursuit of its mission to advance taxpayer rights. The Center's LITC is also hampered in its ability to advise its clients by the double bind that the Internal Revenue Code and Data Policy create—an "intolerable situation that undermines [the Center's] ability to develop trusting relationship with [its] clients and to effectively represent them." *Id.* ¶ 47. Organizations have standing to challenge and are irreparably harmed by rules that interfere with counsel's ability to provide services to their clients–including immigrant clients. *See Cath. Legal Immigr. Network, Inc. v. EOIR*, 2021 WL 184359, at *175 (D.D.C. 2021) (finding that a rule that would "interfere with the[ir] ability … to provide essential services to their clients and/or members—in some cases irretrievably so," constituted irreparable harm); *see also, e.g.*, *Cap. Area Immigrants' Rts. Coal. v. Trump*, 471 F. Supp. 3d 25, 38-9 (D.D.C. 2020) (finding standing and enjoining rule that "will frustrate [plaintiff legal services organizations'] ability to provide legal services directly to asylum applicants, a core component of their respective missions"). Similar obstacles face the Center's LITC Connect members. Olson Decl. ¶ 55-68.

These harms to the Center's ability to engage these populations through its counseling and educational efforts are time sensitive. The tax system operates under strict deadlines for taxpayers, including to file returns and to engage with audits and other requests for information from the IRS, and once a taxpayer misses these deadlines, they lose rights and potentially incur penalties. Olson Decl. ¶ 81-89. This frustration of mission in a time-bound context is similar to

other instances in which courts have found irreparable harm to organizations. *See League of United Latin Am. Citizens v. Exec. Off. of the President*, No. 25-0946, 2025 WL 1187730, at *41 (D.D.C. Apr. 24, 2025); *League of Women Voters*, 838 F.3d at 9; *League of Women Voters of N. Carolina v. North Carolina*, 769 F.3d 224, 247 (4th Cir. 2014) ("once the election occurs, there can be no do-over and no redress"). As with voter registration efforts at issue in those cases, frustration of the Center's efforts to reach, educate, and support taxpayers in applying for ITINs, filing their tax returns, and otherwise engaging with IRS processes to protect their rights and interests, before the relevant deadlines pass, cannot be restored later by Court order.

Second, a sudden and significant erosion of trust in the tax system, based on implementation of the Data Policy, and resulting harm to CTR's mission is irreparable. Olson Decl. ¶ 52-53 ("it is very difficult to restore that trust"). The IRS has acknowledged this, noting that "[i]f the IRS abused [taxpayers'] reasonable expectation of privacy, the resulting loss of public confidence could seriously impair the tax system."[59] This erosion of trust will frustrate the Center's efforts to advance its mission. Olson Decl. ¶ 53 ("[I]f these disclosures continue to go through, trust in the system will further plummet, creating almost insurmountable obstacles to our mission of promoting trust in the system and encouraging participation.").

[59] IRS, Chief Counsel of Procedure & Administration, IRS Pub. 4369, Disclosure & Privacy Law Reference Guide, at 1-9, https://perma.cc/K2JX-89TR. *See also* Bernie Becker & Myah Ward, *IRS Upheaval Cracks Agency Resistance to Data Sharing with Immigration Officials,* Politico (Mar. 31, 2025), https://perma.cc/NQ6Y-ZXPB (noting view of former IRS commissioner under President George W. Bush that disclosures of this type are "a bad trade in the long run," and would result in a "longer-term decline in tax compliance from immigrant communities, and perhaps others who depend on keeping their information filed with the IRS private.").

B. The Center's LITC Clients and Plaintiffs' Members also face imminent, irreparable injury, in the absence of a stay

Taxpayers at imminent risk of having their return information indiscriminately shared with ICE also face irreparable injury. These individuals include clients of the Center's LITC and members of MSA, whose interests these Plaintiffs represent in this action. First, the disclosure of confidential information outside the IRS—in violation of the statutory protections designed to prevent it and without adequate safeguards against further illegal sharing or use—is itself an irreparable injury. Unlawful disclosures of confidential information warrant entry of a preliminary injunction where there is an imminent risk of public disclosure or impermissible use. *See AFL-CIO. v. Dep't of Lab.*, 2025 WL 1783899, at *12 (D.D.C. June 27, 2025) (collecting cases). This is because "the disclosure of private, confidential information 'is the quintessential type of irreparable harm that cannot be compensated or undone by money damages.'" *Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467, 499 (S.D.N.Y. 2019). "Obviously, once … highly personal information is disclosed …, the revelation cannot be undone." *NTEU v. Dep't of Treasury*, 838 F. Supp. 631, 640 (D.D.C. 1993); *see also Hosp. Staffing Sols. v. Reyes*, 736 F. Supp. 2d 192, 200 (D.D.C. 2010) ("the disclosure of confidential information can constitute an irreparable harm because such information, once disclosed, loses its confidential nature."). As addressed in Plaintiffs' Opposition to Defendants' Motion to Dismiss (ECF No. 27), such injuries are also concrete enough to satisfy the requirements of Article III standing because they have "a close historical or common-law analogue," *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021): the torts of intrusion upon seclusion, see *All. for Retired Ams. v. Bessent*, 770 F. Supp. 3d 79, 102 (D.D.C. 2025), and breach of confidence, *see Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1064 (D.C. Cir. 2019).

Further, where such disclosures violate statutorily guaranteed privacy protections for the purpose of supporting criminal investigations or immigration enforcement activity, the violation is more analogous to a deprivation of Fourth Amendment rights than to a violation of an individual's personal privacy. "It has long been established that the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury.'" *Mills v. D.C.*, 571 F.3d 1304, 1312 (D.C. Cir. 2009). For example, in *Klayman v. Obama*, the court found irreparable injury and issued a preliminary injunction where the government was conducting bulk collection of metadata associated with phone calls, allegedly in violation of the Fourth Amendment. 142 F. Supp. 3d 172 (D.D.C. 2015). The court reasoned that where the government violated rights guaranteed to the plaintiffs by the Fourth Amendment, even for a finite time, "the loss of constitutional freedoms is an 'irreparable injury' of the highest order. *Id*. at 181. Such harm likewise occurs when people are forced to provide the information to the government themselves, as taxpayers are required to do under the Internal Revenue Code. *See NTEU*, 838 F. Supp. at 640 (finding irreparable injury "when plaintiffs are forced to choose between revealing constitutionally protected information . . . at the cost of possible further discipline or discharge").

Here, Plaintiffs demonstrate an imminent risk that their members' and clients' data will be broadly disclosed and impermissibly used as a result of the IRS's disclosures. As detailed in, *supra*, Section V.B., ICE's *en masse* data requests are facially noncompliant with the requirements of Section 6103, and the Administration has clearly stated its intention that ICE use the data for an impermissible purpose: to implement "President Trump's promise to carry out the mass deportation of criminal illegal aliens." Ex. 3. Once the IRS shares the data outside the agency, there are no adequate safeguards against subsequent unlawful use or disclosure of the

confidential information. This is not a situation where, for example, data is only being shared among employees within an agency who are obligated to keep it confidential (*All. for Retired Americans v. Bessent*, 770 F. Supp. 3d 79 (D.D.C. 2025); *Univ. of Cal. Student Ass'n v. Carter*, No. 25-cv-0354, 766 F. Supp. 3d 114, 121 (D.D.C. Feb. 17, 2025)) or where there is no evidence that the recipient of the shared data will misuse it or disclose it without authorization (*Baker DC v. Nat'l Lab. Rels. Bd.*, 102 F. Supp. 3d 194, 203 (D.D.C. 2015). Here, the IRS is sharing data with an unknown number of personnel at another agency, and there is significant evidence to support an inference of current and future misuse of the data.

Although there are some safeguards set forth on the face of the MOU and in Section 6103 itself, ICE's and the White House's recent conduct demonstrate material noncompliance with those safeguards. ICE sent a mass request, during the first week of August 2025, seeking personal information for as many as 1.23 million people. As discussed above, given the scale of this request, ICE could not have identified in its request the specific personnel who are "personally and directly engaged in" each one of this many purported investigations, meaning that subsequent disclosure of this confidential information to *other* individuals who will actually carry out any actions ICE plans to take is all but certain. Such subsequent disclosure of the data violates Section 6103(i)(2) (authorizing disclosure of information "solely for the use of such officers and employees in such preparation, investigation, or grand jury proceeding"). And ICE's subsequent misuse of the confidential information seems imminent, given the Administration's stated intention to use the data to support "mass deportation," a civil immigration enforcement function that is not permitted under either the MOU or Section 6103(i)(2).

The White House's conduct further illustrates the risk of noncompliance with the safeguards set forth in the MOU and under Sec. 6103 and the imminence of additional data

sharing. As discussed above, when ICE received less information than expected, in response their mass request, the White House intervened with the IRS directly and asked for more information about these taxpayers, beyond even what was authorized in the MOU and by law.[60] After the IRS declined this request, citing taxpayer privacy rights, then-Commissioner Long was removed.

In addition to the irreparable harm inherent in the disclosures of this confidential information, there are additional imminent, foreseeable consequences to the IRS's indiscriminate data sharing with ICE that cannot be remedied later, if it is allowed to proceed.

Defendants' conduct—handing over confidential home addresses of taxpayers to ICE, in violation of law—places those taxpayers and their family members at imminent risk of the kinds of immigration detention- and removal-related harm that other courts have found warranted preliminary injunctions to prevent, including risk of removal to a third country (*Doe v. Noem*, No. 3:25-cv-00023, 2025 WL 1399216, at *11 (W.D. Va. May 14, 2025)) and risk of summary removal without due process (*D.B.U. v. Trump*, No. 1:25-cv-01163-CNS, 2025 WL 1304288, at *9 (D. Colo. May 6, 2025)), as evidenced by the actual summary removal of an immigrant—*in error*, and contrary to an Immigration Court order forbidding removal—to a notorious prison in a foreign country (*Noem v. Abrego Garcia*, No. 24A949, 2025 WL 1077101 (April 10, 2025)). Plaintiffs' immigrant clients are rightfully frightened of the very real and irreparable harms they face, if the IRS provides their home addresses to ICE.

But taxpayers have more to contend with, under the Data Policy, than "mere fear." *Kirwa v. United States Dep't of Def.*, 285 F. Supp. 3d 21, 43 (D.D.C. 2017). The risks caused by the IRS's radical policy shift and unlawful data sharing with ICE also impede taxpayers' ability to

[60] Jacob Bogage & Kadia Goba, *IRS, White House Clashed Over Immigrants' Data Before Tax Chief Was Ousted*, Wash. Po. (Aug. 9, 2025), https://perma.cc/8SWF-54XS.

safely participate in the tax system—as they are required to do by law and as is necessary to obtain certain benefits to which they are entitled, such as to receive a refund of excess tax withholdings or a credit on behalf of a U.S. citizen child—and to participate in other parts of the formal economy, such as by opening a bank account or borrowing money. Olson Decl. ¶ 73.[61] These rights and obligations are time sensitive; if taxpayers do not timely file their returns or respond to IRS audits and inquiries, they forfeit rights or money to which they would otherwise have been entitled. Olson Decl. ¶ 81-89. Here, as in *Kirwa*, the IRS unlawfully changed a policy and reneged on a promise, putting people who relied on that promise at risk of deportation and in a position where they cannot receive benefits to which they would have otherwise been entitled, demonstrating irreparable harm. *Id*. at 42-43.

Together, the violation of taxpayers' statutory privacy rights and its real-world consequences demonstrate concrete, imminent irreparable harm. The White House and DHS demanded in June 2025 that the IRS assist ICE in locating as many as 7.3 million immigrants, *see* Ex. 3—more than the total number of active U.S. ITIN holders (immigrant taxpayers).[62] This request led to the ouster of the Acting IRS Chief Counsel when he refused, and the IRS and ICE subsequently developed an automated process for receiving and responding to bulk-requests. See Ex. 3. The IRS has now reportedly shared home address information in bulk for tens of thousands of people. And—when asked about the White House's reported displeasure that more data was not disclosed and the ouster of the IRS Commissioner—a the White House stated that Administration officials were "aligned on the mission" to "eliminate[ ] information silos." Ex. 1.

[61] *See also* Lauren Kaori Gurley & Jacob Bogage, *Deportation Fears Trigger Decline in Tax Filings in Immigrant Communities,* Wash. Po. (May 19, 2025), https://perma.cc/49WU-FQ86.
[62] Treasury Inspector Gen. for Tax Admin., Administration of the Individual Taxpayer Identification of Number Program (2023), at 1, https://perma.cc/H52Q-7ZU5 (5.8 million active ITIN numbers as of Dec. 31, 2022).

The irreparable harm of the privacy violation has already arrived, for the tens of thousands of taxpayers whose data has already reportedly been disclosed, and these harms are plainly imminent for the remaining ITIN holders, who are among the LITC's clients, Olson Decl. ¶ 13, 17, 42, and MSA's members, Phetteplace Decl. ¶ 9. Moreover, the fear of detention- and removal-related harms and the associated impediments to safely engaging with the IRS and the tax system cause irreparable harms to taxpayers who are themselves at risk of ICE enforcement or share a household with those who are, including those among the LITC's clients, *see*, *e.g.*, Olson Decl. ¶ 48-49, and MSA's members, Phetteplace Decl. ¶ 6-8, 12-14.

III. Balance of the Equities

"It is well established that the Government cannot suffer harm from [relief] that merely ends an unlawful practice." *C.G.B. v. Wolf*, 464 F. Supp. 3d 174, 218 (D.D.C. 2020) (internal quotation marks and citations omitted). Likewise, "[t]here is generally no public interest in the perpetuation of unlawful agency action." *Open Cmtys. All. v. Carson*, 286 F. Supp. 3d 148, 179 (D.D.C. 2017) (citing *League of Women Voters of United States v. Newby*, 838 F.3d 1, 12 (D.C. Cir. 2016)). "To the contrary, there is a substantial public interest in having governmental agencies abide by the federal laws—such as the APA. . .—that govern their existence and operations." *Id.* (internal quotation marks and citations omitted). Thus, for the same reasons that Plaintiffs are likely to succeed on the merits, equity requires relief.

But even if this Court were to balance Defendants' interests as if it were a private party, the balance of equities and public interest would still overwhelmingly favor Plaintiffs. Neither Defendants, nor any non-defendant component of the Government, have any lawful or legitimate need to unlawfully share the personal data of millions of taxpayers from one of the government's most sensitive systems.

IV. The Court Should Stay the Data Policy under Section 705

A stay of Defendants' Data Policy is the appropriate preliminary relief to preserve the status quo ante while this case proceeds. Section 705 of the APA allows a court to "postpone the effective date of an agency action or . . . preserve status or rights pending conclusion of the review proceedings." 5 U.S.C. § 705. "Courts—including the Supreme Court—routinely stay already effective agency action." *Texas v. Biden*, 646 F. Supp. 3d 753, 770 (N.D. Tex. 2022) (citing, e.g., *W. Virginia v. EPA*, 577 U.S. 1126 (2016)); *accord Kingdom v. Trump*, No. 25-cv-691, 2025 WL 1568238, at *5 (D.D.C. June 3, 2025) (observing that "various courts have interpreted § 705 to permit a 'stay'— which may be more aptly described as a temporary rollback—even of already-consummated agency action"); see also *Trump v. CASA*, 2025 WL 1773631, at *2567 (2025) (Kavanaugh J., concurring) ("in cases under the Administrative Procedure Act," courts may "preliminarily 'set aside'" an agency action). Accordingly, the fact that the policy is "already in effect does not bar this Court from staying [it]—and returning things to the status quo ante while this case proceeds—under section 705." *Coal. for Humane Immigr. Rts.*, 2025 WL 2192986, at *15.[63]

CONCLUSION

For all these reasons, the Court should grant Plaintiffs' motion and enter a stay under section 705, preliminary set aside the agency action under section 706, or preliminarily enjoin Defendants actions.

Dated: August 20, 2025

Respectfully submitted,

/s/ Johanna M. Hickman

[63] In the alternative, the Court should issue a preliminary injunction. Plaintiffs respectfully request that it either waive or set only a nominal bond requirement under Fed. R. Civ. P. 65(c).

Daniel A. McGrath (D.C. Bar No. 1531723)
Johanna M. Hickman (D.C. Bar No. 981770)
Madeline H. Gitomer (D.C. Bar No 1023447)
Robin Thurston (D.C. Bar No. 1531399)
Steven Y. Bressler (D.C. Bar No. 482492)
Democracy Forward Foundation
P.O. Box 34553
Washington, DC 20043
202-448-9090
dmcgrath@democracyforward.org
hhickman@democracyforward.org
mgitomer@democracyforward.org
rthurston@democracyforward.org
sbressler@democracyforward.org

Counsel for Plaintiffs