March 6, 2026

Ryan Law
Deputy Assistant Secretary for Privacy, Transparency, and Records
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Re: Comments Proposed System of Records Notice, Department of the Treasury, Departmental Offices DO .0197—Financial Assistance Programs (FR Doc. 2026-02234)

We respectfully submit these comments on behalf of UnidosUS and Citizens for Responsibility and Ethics in Washington (CREW).

UnidosUS is the nation's largest Latino civil rights and advocacy organization, representing nearly 300 affiliated community-based organizations serving millions of Latino families across 37 states, Washington, D.C., and Puerto Rico. For more than 55 years, UnidosUS has advanced economic opportunity for Latino families and worked to ensure that America's promise is open to all who contribute to its strength, including U.S. citizens by birth, naturalized citizens, lawful permanent residents, and other members of our communities whose personal information will be directly affected by the modifications proposed in this system of records notice (SORN).

Our affiliated organizations were on the front lines of administering and connecting families to the programs now encompassed by this SORN. UnidosUS affiliates helped Latino families navigate applications for Emergency Rental Assistance, the Homeowner Assistance Fund, and the State Small Business Credit Initiative programs during some of the most acute economic distress in recent memory. The families we serve disclosed their most sensitive personal and financial information—Social Security numbers, individual taxpayer identification numbers, household income, family composition, addresses, and employment records—to those programs in good faith, in reliance on explicit and implicit representations that their data would be protected and used only for the purpose for which it was collected: to determine their eligibility for urgently needed housing and economic relief.

CREW is a nonprofit, nonpartisan watchdog organization dedicated to promoting integrity, transparency, and accountability in government. As part of its mission-critical work, CREW monitors and identifies potential governmental abuses of Americans' sensitive personal data. Ensuring Executive Branch compliance with the Privacy Act and its public participation and transparency requirements are activities central to CREW's mission. CREW staff have demonstrated expertise in federal government information laws, including the Privacy Act and Paperwork Reduction Act.

We oppose this SORN in its entirety. What Treasury published is far from a routine administrative record-keeping notice. It is an attempt to consolidate sensitive personal data collected across multiple, Congressionally authorized programs into a single unified federal system. As legal authority, it relies on an Executive Order that purports to make data available

for cross-agency sharing, including for immigration enforcement, in a manner that the underlying program statutes do not authorize, Privacy Act does not permit, and Constitution does not allow.

This is, in the clearest sense, a betrayal of the trust that vulnerable families placed in their government when they sought the assistance that they were legally entitled to receive. The concept of "data betrayal" describes a specific and legally cognizable harm: the government's repurposing of information that individuals were compelled or strongly induced to disclose for one purpose—qualifying for benefits—against the same people for an entirely different and adverse purpose.

The Privacy Act was enacted precisely to prevent this. Every element of this proposed system of records notice, including the consolidation of separately authorized program data, overbroad routine uses, reliance upon EO 14243, and absence of any program-by-program analysis, confirms that data betrayal is not an incidental risk, but the chief objective of this proposal. This purpose is impermissible.

The legal deficiencies of this notice are numerous, serious, and independently sufficient to require its withdrawal.

- The SORN's deficiencies include it title, "Financial Assistance Programs," which is itself inadequate. OMB Circular A-108, which requires that a system name accurately describe the system's true function. The name implies that Treasury is administering or providing financial assistance; in reality, as the body of the notice makes clear, the system's function is to aggregate, audit, and redistribute data about the recipients of such assistance to a broad array of other agencies and entities. This misdescription is not cosmetic. It is the first in a series of framings designed to obscure the system's actual purpose from the individuals whose data it will hold.
- Treasury cites an Executive Order, which cannot override a statute as legal authority, as a legal basis for this system notice.
- The proposed routine uses are not compatible with the purposes for which data was collected, as the Privacy Act requires.
- The consolidation of data from separately authorized programs is a substantive policy change that requires notice-and-comment rulemaking under the Administrative Procedure Act, not a SORN.
- The system as proposed conflicts with Section 6103 of the Internal Revenue Code, which strictly prohibits the repurposing of tax-related financial information, and which federal courts have twice recently held prohibits precisely the kind of cross-agency data sharing this system contemplates.
- The system fails to satisfy multiple specific mandatory requirements of the Privacy Act itself, including requirements of notice at collection, accuracy, specificity of routine uses, security safeguards, and—if automated cross-referencing is contemplated—Computer Matching Agreement procedures.

The communities that UnidosUS represents include many mixed-status households, or families where some members are citizens or lawful permanent residents and others are undocumented, who made careful and often agonizing decisions to seek emergency rental assistance or homeowner relief during the COVID-19 pandemic and its economic aftermath. These families

did so in reliance on federal laws and policies that protected the privacy of their data. They are entitled to insist that government policies, and promises, that preserve privacy are honored under law. The proposed system of records breaks that trust.

UnidosUS and CREW strongly oppose this SORN and urge the Treasury to immediately withdraw this notice, cease any cross-program data consolidation that may already have begun, and abandon this proposal. No mere revision of this proposal could be made legally sufficient.

The SORN Contains Numerous Serious Legal Deficiencies

This comment sets forth the following objections to the proposed system of records:

- First, Executive Order 14243, "Eliminating Information Silos," which was cited as legal authority for this notice, cannot override the Privacy Act's mandatory prohibitions on incompatible disclosures. An executive order cannot amend a statute. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).
- Second, the consolidation of data from multiple separately authorized federal assistance programs into a single system of records is a substantive policy change requiring notice-and-comment rulemaking under the Administrative Procedure Act, 5 U.S.C. § 553. A SORN is inadequate.
- Third, the proposed routine uses are incompatible with the purposes for which data was collected, as required by 5 U.S.C. § 552a(b)(3), and Treasury has provided no program-by-program compatibility analysis as required by OMB Circular A-108.
- Fourth, the underlying program statutes—including 15 U.S.C. §§ 9058a and 9058d, 42 U.S.C. §§ 802–805, and others—independently constrain how associated data may be used. Congress did not authorize immigration enforcement uses of data collected under these programs, which serve an entirely distinct purpose.
- Fifth, the proposed system conflicts with Section 6103 of the Internal Revenue Code, 26 U.S.C. § 6103, which strictly prohibits repurposing tax-related financial information. Two federal courts have recently enjoined the Administration's IRS-ICE data sharing on these grounds.
- Sixth, the SORN violates five specific mandatory requirements of the Privacy Act: the notice-at-collection requirement (§ 552a(e)(3)), the specificity requirement (§ 552a(e)(4)(D)), the accuracy requirement (§ 552a(e)(5)), the security safeguards requirement (§ 552a(e)(9), (e)(10)), and the Computer Matching Agreement requirement (§ 552a(o)) if automated cross-referencing is contemplated.
- Seventh, the proposed system will cause concrete, foreseeable, and irreparable harm to Latino and mixed-status families who disclosed their most sensitive personal and financial information in reliance on the government's implicit and explicit commitments to protect it. This is the definition of data betrayal, and it causes legally cognizable injury independent of any downstream enforcement action.
- Eighth, the data collection that Treasury proposes to conduct through this system, including gathering records from states, localities, and other grantees across eight distinct programs covering millions of individual beneficiaries, constitutes a "collection of information" subject to the Paperwork Reduction Act, 44 U.S.C. §§ 3501 (PRA). Because this collection is directed at a class of recipients rather than specific individuals under audit, it requires OMB review, public notice, and an assigned OMB Control Number. Treasury has obtained none of these. Under the PRA's public protection clause,

44 U.S.C. § 3512, grantees and other entities from whom information is sought are not required to comply with a collection that lacks an OMB Control Number. Treasury's failure to comply with the PRA is an independent basis for withdrawal of this notice and for cessation of any data collection already underway.

I. BACKGROUND: THE PRIVACY ACT WAS ENACTED TO PREVENT CENTRALIZED FEDERAL DATA BANKS AND UNAUTHORIZED DISCLOSURE

A. The Privacy Act's Core Purpose and Legislative History

The Privacy Act of 1974 was enacted by Congress in direct response to documented abuses of federal government power during the Watergate scandal and the FBI's COINTELPRO program, during which federal agencies secretly and illegally compiled dossiers on American citizens deemed "subversive" and used personal information for unauthorized purposes. Congress acted to ensure that what was then called the "Information Age" would not become an instrument of government surveillance and control. The Act's core purpose was to guarantee that information individuals provide to the government for one defined purpose cannot be turned against them for another.

The legislative history is explicit on this point. As the U.S. Senate Committee on Government Operations' 1976 Source Book on Privacy explains, the Privacy Act was designed to prevent "formal or de facto national data banks" or "centralized Federal information systems" that could consolidate sensitive personal data stored across separate agencies. Congress established "robust safeguards against such 'interagency computer data banks' to make it 'legally impossible for the Federal Government in the future to put together anything resembling a '1984' personal dossier on a citizen.'"

Treasury's proposed system of records is precisely the kind of centralized federal information system that Congress enacted the Privacy Act to prohibit. It consolidates data from at least eight separately authorized federal assistance programs into a single unified repository and proposes routine uses that would make that consolidated data available to other federal agencies, law enforcement, contractors, and researchers—without any demonstration that such uses are compatible with the purposes for which the data was originally collected. This is not a technical administrative matter. It is an attempt to create, through a system of records notice, the kind of interagency data bank that Congress has repeatedly and specifically prohibited.

The consolidation Treasury proposes also independently fails the requirements of OMB Circular A-108 (2016), which governs how agencies structure systems of records. That guidance requires agencies to weigh five specific considerations before combining records from separate programs into a single system, including whether the combined system effectively facilitates the exercise of individual rights under the Privacy Act. The programs covered by this SORN do not share common authorities, purposes, categories of individuals served, security and access safeguards, or routine uses. Routine uses, in particular, must flow from the specific statutory purpose of each program's authorizing legislation; they cannot be generalized across a collection of programs with fundamentally different statutory frameworks. Treasury has not conducted or published any

analysis of the OMB Circular A-108 criteria. Its failure to do so is an independent basis for withdrawal.

The proposed system also constitutes a paradigmatic act of data betrayal: the government is proposing to take information that millions of vulnerable families disclosed under economic duress, in reliance on representations that it would be used to help them, and consolidate it into a system designed to be shared with agencies whose purposes are adverse to those families. The breach of trust is structural and not incidental.

B. The Computer Matching and Privacy Protection Act Separately Prohibits this Consolidation

Congress reinforced the Privacy Act's prohibition on centralized data systems by enacting the Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503, codified at 5 U.S.C. § 552a(o). That statute requires that when agencies engage in automated comparison of records across systems—*i.e.*, "computer matching"—they must execute written matching agreements containing specific safeguards, obtain review by a Data Integrity Board, and include cost-benefit analysis demonstrating the program is "likely to be cost effective." These requirements exist precisely because Congress recognized that cross-agency data matching poses unique risks to individual privacy that the original Privacy Act framework was not designed to address.

Treasury has published no Computer Matching Agreement in connection with this proposed system of records. Yet the broad routine uses proposed—including disclosure to federal agencies for fraud detection, law enforcement referrals, and statistical analysis—plainly contemplate automated cross-referencing of beneficiary records across programs and against other federal datasets. If automated matching is contemplated, as the routine uses strongly suggest, a Computer Matching Agreement is a legal prerequisite that Treasury has not satisfied. This is an independent and sufficient basis for withdrawal of this notice.

C. The Privacy Act's Mandatory Substantive Requirements

The Privacy Act imposes specific, mandatory substantive requirements on any agency maintaining a system of records. Treasury's proposed SORN fails multiple requirements, each of which constitutes an independent legal deficiency. The following summarizes the applicable requirements, and below we address each violation in detail.

Compatible Use Requirement. Agencies may only disclose records in a "routine use" if that use is "compatible with the purpose for which [the information] was collected." 5 U.S.C. § 552a(a)(7), (b)(3). OMB Circular A-108 (2016) requires agencies to explain how each proposed routine use satisfies this compatibility requirement. The original OMB Privacy Act Implementation Guidelines make clear that "[t]he language [of the Privacy Act] would also seem to imply that the use should be generally related to the purpose for which the record is maintained." Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28,951 (July 9, 1975). Treasury has provided no such analysis.

OMB's Privacy Act Guidelines—issued in 1975 alongside the passage of the Act—reinforce that the Privacy Act's routine use provisions are "intended to discourage the unnecessary exchange of information to other persons or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material." OMB, Privacy Act Guidelines, 40 Fed. Reg. 28949, 28953 (July 1, 1975), https://perma.cc/776J-4L46. Thus, "a 'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained." *Id.* Executive branch interpretations, including OMB's, "issued contemporaneously with the statute at issue, and which have remained consistent over time," may be "especially useful in determining the meaning" of a statute. *Loper Bright Enterprises v. Raimondo, 603 U.S. __, slip op. at 16–17 (2024)*; *see also Maydak v. United States*, 363 F.3d 512, 518 (D.C. Cir. 2004) (relying on OMB's 1975 Privacy Act Guidelines in construing statute).

Notice-at-Collection Requirement. Agencies must inform individuals at the time of collection of the authority, purpose, and routine uses for information collected, and describe the consequences of not providing the requested information. 5 U.S.C. § 552a(e)(3). Millions of applicants for the programs covered by this SORN received no notice that their data could be consolidated into a cross-agency system or used for immigration enforcement.

Specificity Requirement. The Privacy Act requires agencies to publish detailed SORNs in the Federal Register describing what records are maintained, how they are used, and with whom they are shared. Specifically, SORNs must include "each routine use of the records contained in the system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D). OMB's implementing guidance requires that routine use descriptions be "sufficiently specific to allow an individual to make an informed judgment about whether to provide personal information to an agency." *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948, 28,963 (July 9, 1975); *see also* OMB Circular No. A-108, § 6(k) (Dec. 23, 2016) (reaffirming that routine uses "shall be narrowly tailored" and described with "sufficient clarity and specificity").

Accuracy Requirement. Agencies must maintain records used in making determinations about individuals "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual." 5 U.S.C. § 552a(e)(5). Data collected under emergency conditions years ago has not been assessed for accuracy in the proposed new enforcement context.

Security Safeguards Requirement. Agencies must establish "appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records" and prevent "substantial harm, embarrassment, inconvenience, or unfairness." 5 U.S.C. § 552a(e)(10). The proposed system creates materially greater security risk through consolidation, and Treasury has provided no security assessment.

Computer Matching Agreement Requirement. If automated cross-referencing is contemplated, a Computer Matching Agreement including a Data Integrity Board review is required. 5 U.S.C. § 552a(o). No such agreement has been published.

D. A "Panoply of Laws" Beyond the Privacy Act Also Governs These Data

As a federal district court noted in the analogous SSA data-sharing context, SSA's data systems are "subject to a 'panoply of laws' that govern and protect" them, beyond the Privacy Act itself. *Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. Social Security Administration*, No. 1:25-cv-00596-ELH (D. Md. Apr. 17, 2025) (ECF 146). The same is true here.

The data proposed to be consolidated in this system is governed by, at minimum:

- The Privacy Act of 1974, 5 U.S.C. § 552a, including all mandatory requirements described above.
- The underlying program statutes, including 15 U.S.C. §§ 9058a, 9058c, 9058d; 42 U.S.C. §§ 802–805; 12 U.S.C. §§ 5701 et seq.; 33 U.S.C. § 1321 note; and 42 U.S.C. §§ 1397n et seq., each of which authorizes data collection for specific, limited purposes that do not include immigration enforcement or cross-agency data consolidation.
- Section 6103 of the Internal Revenue Code, 26 U.S.C. § 6103*,* which strictly prohibits the disclosure of tax return information and presumes confidentiality except in narrowly drawn, specified circumstances. Much of the eligibility documentation collected under these programs derives from or cross-references IRS records and is therefore subject to § 6103's protections.
- The Federal Information Security Modernization Act (FISMA), 44 U.S.C. §§ 3553–3554, which requires agencies to implement security controls commensurate with the risk and magnitude of harm from unauthorized access, use, or disclosure.
- The Administrative Procedure Act, 5 U.S.C. §§ 553, 706*,* which requires notice-and-comment rulemaking for substantive policy changes and prohibits agency action that is arbitrary, capricious, or contrary to law.

Treasury's compliance obligations encompass all of these authorities. It cannot satisfy the Privacy Act's procedural requirements while ignoring the substantive requirements of the program statutes, § 6103, FISMA, and the APA. The proposed SORN fails under each of these frameworks.

The comprehensive statutory framework governing this data reflects a considered judgment by Congress that certain categories of sensitive personal information—including financial data, tax information, household composition, and income—collected under compulsion or strong inducement in the context of government benefit programs require heightened protection precisely because the power imbalance between the government and the individual is most acute in those settings. When the government uses that imbalance to extract information and then repurposes it against the people who provided it, it commits exactly the kind of data betrayal that these overlapping statutory frameworks were designed to prevent.

II. EXECUTIVE ORDER 14243 DOES NOT FURNISH LEGAL AUTHORITY FOR THIS ACTION

A. Executive Orders Cannot Override Statutes

It is a foundational principle of constitutional law that executive orders derive their legal force from either a specific statutory delegation by Congress or the President's inherent constitutional authority. They cannot override, modify, expand, or contradict the requirements of federal statutes. Where a statute speaks directly to a question, an executive order that conflicts with or seeks to expand its effects beyond that statute is without legal effect.

The Supreme Court established this principle definitively in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952). Justice Jackson's controlling concurrence establishes the governing framework: when the President acts in ways that are "incompatible with the expressed or implied will of Congress," his power is "at its lowest ebb," and courts may sustain his actions only on the basis of his own constitutional authority minus any constitutional powers of Congress over the matter. *Id.* at 637–38 (Jackson, J., concurring). The Privacy Act contains specific, mandatory prohibitions on disclosure. The President cannot amend it, waive its requirements, or expand the authorized exceptions to it via executive order.

This is not a close question. The Privacy Act commands that agencies "shall not disclose" records except in enumerated circumstances, 5 U.S.C. § 552a(b), and that routine uses must be "compatible with the purpose for which [the information] was collected," 5 U.S.C. § 552a(7)). These are mandatory statutory commands. An executive order directing broader data sharing—whatever its stated rationale—does not and cannot modify these commands.

B. What Executive Order 14243 Is and What It Does

Executive Order 14243, "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos," was signed by President Trump on March 20, 2025, 90 Fed. Reg. 13681 (Mar. 25, 2025). It directs federal agency heads to take "all necessary steps, to the maximum extent consistent with law," to ensure that designated federal officials have "full and prompt access to all unclassified agency records, data, software systems, and information technology systems." Within 30 days of publication, agency heads were tasked with rescinding or modifying agency guidance that limits intra- or inter-agency data sharing and submit a report to OMB recommending whether agency regulations—including SORNs—should also be eliminated or modified. Most significantly, EO 14243 directs agencies to ensure that "the Federal Government has unfettered access to comprehensive data from all State programs that receive Federal funding, including, as appropriate, data generated by those programs but maintained in third-party databases."

The order's stated purpose is "eliminating bureaucratic duplication and inefficiency while enhancing the Government's ability to detect overpayments and fraud." That language is repeated in proposed Routine Use (2) of this SORN, which authorizes disclosure for "identification and prevention of fraud, waste, and abuse." EO 14243 is therefore an attempt to create administrative infrastructure for the data consolidation and cross-agency sharing program that this SORN attempts to implement.

The weakness of EO 14243 as a legal authority is compounded by the inadequacy of the other authorities that Treasury cites. An examination of the full list reveals a pattern of citation that obscures rather than supports Treasury's legal basis for this collection. 44 U.S.C. § 3101, the general federal records management statute, governs agency obligations once records already

exist; it does not authorize the creation or collection of records and cannot serve as authority for this system. 44 U.S.C. § 3554, the Federal Information Security Modernization Act (FISMA) provision on security controls, similarly governs the protection of records once held. It is not a collection authority and has never been treated as one.

Most significantly, Treasury omits from its list of cited authorities the provision it is most likely actually relying upon to compel production of records from grantees: 2 C.F.R. § 200.337, the record retention and audit access provision, which gives federal agencies and their representatives the right of access to grantee records pertinent to a federal award. This omission is telling. Section 200.337 is not an unlimited access right and it includes specific limitations, including that agencies and their representatives "must take measures to protect the name of victims of a crime when access to the victim's name is necessary." None of those limitations appear anywhere in this SORN, because Treasury has not acknowledged § 200.337 as its operative authority. An agency that conceals its actual legal theory from the public cannot claim to have satisfied its obligation of transparency under the Privacy Act or the APA.

The administration has been explicit about EO 14243's downstream purposes. Reporting and court records that EO 14243 is being used to facilitate immigration enforcement by making benefit program data, tax data, and Social Security data available to DHS and ICE. *California v. Rollins*, No. 3:25-cv-06310-MMC, Doc. 134 (N.D. Cal. Feb. 26, 2026) (order granting in part motion for preliminary injunction). The inclusion of EO 14243 as a cited legal authority in this Treasury SORN is a declaration of intent: it is evident that this system is being built, at least in part, to serve the data consolidation agenda that EO 14243 is designed to advance.

C. EO 14243 Cannot Authorize Disclosures That Violate the Privacy Act

Treasury's citation of EO 14243 as legal authority for this system is legally indefensible on its face. An executive order cannot waive or modify the Privacy Act's mandatory prohibition on incompatible disclosures. It cannot expand the universe of permissible routine uses beyond what 5 U.S.C. § 552a(b)(3) allows. It cannot override the specific statutory purposes embedded in the Congressional appropriations funding these programs. It also cannot create new disclosure authority that Congress has not granted.

Courts Have Repeatedly Rejected the Administration's Broad Data-Sharing Theory

The courts have not been passive observers of this administration's effort to use executive orders to override statutory data protections. In the IRS-ICE data sharing context, which is both analogous and relevant to what is proposed here, two federal district courts have issued injunctions blocking data sharing that the administration justified in part by reference to its executive authority.

In *Community Economic Development Center of Southeastern Massachusetts et al. v. Bessent et al.*, U.S. District Court for the District of Massachusetts (Feb. 5, 2026), Judge Indira Talwani issued a preliminary injunction finding that the IRS-ICE data sharing arrangement likely violated Section 6103 of the Internal Revenue Code. The court found that plaintiffs demonstrated a "high likelihood" that ICE's use of taxpayer data "violated and continues to violate" the Internal

Revenue Code—notwithstanding the administration's assertion that its executive authority authorized the arrangement.

In *Center for Taxpayer Rights et al. v. Internal Revenue Service et al.*, No. 1:25-cv-00457 (D.D.C.), Judge Colleen Kollar-Kotelly similarly enjoined IRS data sharing with DHS and ICE, finding the administration's "Address-Sharing Policy" unlawful under § 6103 and arbitrary and capricious under the APA.

D. Citation of EO 14243 Reveals the Intended Purpose of this System

Inclusion of EO 14243 in the authorities section signals that Treasury is positioning this consolidated system to be usable for the cross-agency data sharing—including immigration enforcement data sharing—that EO 14243 was designed to facilitate. Treasury has not explained any other reason for citing an immigration-adjacent executive order as authority for a financial assistance data system.

This goes to the question of compatible use. The Privacy Act requires that routine uses be compatible with original collection purposes. If the evident purpose of this system is to make housing and economic relief program data available for immigration enforcement—as the citation of EO 14243 strongly suggests—that purpose is incompatible with the purpose of housing and economic relief programs.

It also matters because it illuminates the nature of the harm. Families who disclosed their most sensitive personal and financial information to qualify for emergency rental assistance or homeowner relief did so in a context defined by urgency and by the government's representations that the information would be used to help them. Citing an immigration enforcement executive order as authority to consolidate that data is not merely a legal error. It is a declaration that the data collected in a relationship of trust will be used to betray that trust.

Treasury should withdraw this notice, remove EO 14243 from the listed legal authorities, and demonstrate—if it reissues any version of this notice—that each proposed routine use is independently authorized by a specific statute and is compatible with the original collection purposes of each program whose data would be included in the system. A presidential directive to share data "to the maximum extent consistent with law" is not a legal authority for any specific disclosure. Only Congress can create the authority that Treasury is attempting to claim through this SORN.

III. POSSIBLE CONSOLIDATION OF THESE PROGRAM DATASETS REQUIRES APA NOTICE-AND-COMMENT RULEMAKING, NOT A SORN

A. The APA Requires Rulemaking for Substantive Policy Changes Affecting Rights and Obligations

The Administrative Procedure Act requires notice-and-comment rulemaking when agencies make substantive policy changes affecting rights and obligations. 5 U.S.C. § 553. An agency cannot evade this requirement by characterizing a substantive policy change as a procedural or

administrative matter. The determinative question is whether the agency action has the force and effect of law—whether it creates new rights and obligations, alters existing relationships, or affects the legal interests of individuals in a substantial way.

B. This Consolidation Is a Major Policy Change of the First Magnitude

Treasury's proposed system of records—despite its packaging in a SORN—is not a routine administrative update. It proposes to consolidate data from at least eight separately authorized federal assistance programs into a single unified federal system with broad new disclosure authorities. Yet these programs were enacted by Congress for specific, limited purposes, administered through a complex web of state, local, and tribal government partners, and used by millions of Americans who disclosed sensitive personal and financial information in the context of each program's specific statutory framework. No single SORN can satisfy the Privacy Act's mandatory requirements simultaneously for this range of programs. Treasury has not attempted to show otherwise.

Under the existing program-specific frameworks, data collected for the Emergency Rental Assistance program is governed by the purposes and constraints of that program. Data collected for the Homeowner Assistance Fund is governed by that program's statutory framework. Data collected for the State Small Business Credit Initiative is governed by that program's authorizing statute. These reflect distinct congressional judgments about who should receive what kind of assistance under what conditions, and about the privacy expectations of those who sought that assistance.

The programmatic diversity of the covered programs illustrates precisely why single-system consolidation fails the OMB Circular A-108 criteria. These programs range from emergency rental assistance for families facing eviction, to Gulf Coast environmental and economic recovery grants, to complex pay-for-results demonstration projects evaluating social interventions. They operate under different appropriations statutes, serve different beneficiary populations, use different eligibility criteria, and were administered through different governmental and non-governmental structures. They do not share common authorities, purposes, categories of individuals, or security and access requirements. Routine uses, which must be compatible with each program's unique statutory purpose, cannot be generalized across programs with such fundamentally different authorizing frameworks without violating the compatibility requirement with respect to at least some, and likely all, of the programs included.

By collapsing these separately authorized systems into a single consolidated repository, Treasury is making a major policy decision that affects the legal rights of millions of individuals, requires reconciliation of multiple conflicting statutory authorities, and contradicts the terms and representations under which data was originally collected. This is precisely the kind of major policy change that requires APA rulemaking.

The Supreme Court's arbitrary-and-capricious standard reinforces this conclusion. Under *Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Automobile Insurance Co.*, 463 U.S. 29, 43 (1983), agency action is arbitrary and capricious if the agency "has relied on factors which Congress has not intended it to consider." Under *Encino Motorcars, LLC v. Navarro*, 579 U.S.

211, 221 (2016), agencies must provide a reasoned explanation for their actions. Treasury has offered no reasoned justification for consolidating data across these distinct programs, no explanation of what statutory authority permits this consolidation, and no analysis of the significant interests of the millions of individuals whose data would be affected.

D. Treasury Must Clarify Whether—and What—Data Consolidation Has Already Begun

This SORN was published on February 3, 2026. The programs it covers, including the Emergency Rental Assistance, Homeowner Assistance Fund, State and Local Fiscal Recovery Funds, and others, have been operational for years. Treasury has not disclosed whether any cross-program data consolidation has already begun under the authority of EO 14243 or otherwise, or whether this SORN is genuinely prospective or is an attempt to retroactively legitimize actions already taken.

This matters for two independent reasons. First, if Treasury has already begun consolidating data from these programs into a unified system, it has been operating an unlawful data-sharing arrangement without any Privacy Act authorization since at least the date of the initial consolidation. The Privacy Act requires notice and a period for public comment before a new system of records becomes effective. If Treasury has already acted, it has already violated the Act.

Second, if data was already consolidated and shared, including, potentially, through the DOGE-related access to Treasury systems documented in related litigation, the harm has already occurred. We therefore demand that Treasury disclose the full timeline of any cross-program data consolidation activity, including any access by DOGE-affiliated personnel, as it is material to the timing and implications of a policy change reflected by the department's actions.

E. The Absence of Reasoned Justification Is Arbitrary and Capricious

Treasury offers no explanation of what legitimate program administration purpose is served by consolidating data from these eight distinct programs into a single system of records. It has not explained why program-specific data management frameworks are insufficient. It has not explained how the proposed consolidation is consistent with the statutory purposes of any of the covered programs. It has not addressed the significant reliance interests of the millions of individuals whose data would be affected. It also appears not to have considered alternatives.

This is not a close case under the arbitrary-and-capricious standard. An agency that proposes a major policy change affecting the legal rights of millions of people, offers no reasoned justification for it, cites as authority an Executive Order that cannot override the applicable statutes, and fails to address the most obvious objections to its proposal, has not satisfied its obligation of reasoned decision-making.

An additional indicator of arbitrariness is the basis on which programs were selected for inclusion in this system. The programs covered by this SORN—the Emergency Rental Assistance programs, the Homeowner Assistance Fund, the State and Local Fiscal Recovery Funds, the Capital Projects Fund, the State Small Business Credit Initiative, the RESTORE Act

programs, SIPPRA, and the Local Assistance and Tribal Consistency Fund—share no single unifying statutory characteristic that would explain their consolidation. Treasury has offered no criteria for program inclusion and no neutral programmatic rationale is apparent from the face of the notice. Under *Motor Vehicle Manufacturers Ass'n v. State Farm*, an agency that "has relied on factors which Congress has not intended it to consider" acts arbitrarily and capriciously. The selection of programs for this system based on criteria that appear to track political provenance rather than programmatic characteristics is precisely the kind of factor Congress did not intend Treasury to consider.

IV. SPECIFIC PROGRAM STATUTES INDEPENDENTLY BAR THE PROPOSED USES

A. The Statutory Purpose of Each Program Constrains How Its Data May Be Used

The financial assistance programs consolidated in this proposed system of records were not created by a single omnibus statute. Each was enacted by Congress for a specific, defined purpose, with a specific beneficiary population in mind, under specific conditions of economic and public health emergency. The data collected under each program carries with it the statutory purpose of the program that authorized its collection. Treasury cannot strip or alter the statutory character of the program data by consolidating it into a unified system.

The Emergency Rental Assistance programs were created under 15 U.S.C. §§ 9058a and 9058c to prevent eviction and housing instability during and after the COVID-19 pandemic. Congress appropriated those funds specifically to keep families in their homes. Data collected in connection with ERA applications—income verification, household composition, landlord information, addresses—was collected for that purpose and that purpose only. Congress was also explicit, in 15 U.S.C. § 9058a(4), that ERA data relating to victims of domestic violence, sexual assault, and stalking must receive heightened privacy protections.

These statutory protections are mandatory conditions on the use of ERA data. The proposed SORN is entirely silent on these requirements. Routine Uses (2) and (4), which authorize disclosure for fraud prevention and law enforcement referrals, could be used to disclose the location and household information of survivors of intimate partner violence, sexual assault, or stalking to law enforcement agencies without any of the statutory protections § 9058a(4) requires. This risk is a direct consequence of Treasury's failure to conduct any program-by-program statutory analysis before proposing consolidated routine uses. The ERA's domestic violence survivor protections constitute an independently sufficient basis for excluding ERA domestic violence victim data from this system and withdrawing the SORN.

The Homeowner Assistance Fund was established under 15 U.S.C. § 9058d to prevent mortgage delinquency, default, displacement, and foreclosure for homeowners experiencing pandemic-related financial hardship. The State and Local Fiscal Recovery Funds and Capital Projects Fund were created under 42 U.S.C. §§ 802–805 to support governmental response to the pandemic and economic recovery. The Local Assistance and Tribal Consistency Fund was established under 42 U.S.C. § 805. The State Small Business Credit Initiative programs operate under 12 U.S.C. §§

5701. The RESTORE Act programs operate under 33 U.S.C. § 1321. The Social Impact Partnership to Pay for Results Act program operates under 42 U.S.C. §§ 1397n.

None of these statutes authorized the collection of beneficiary data for immigration enforcement, cross-agency surveillance, law enforcement referrals, or the kind of centralized federal database Treasury is now proposing to establish. The statutory purposes are specific and limited. Data collected under these programs may only be used for purposes consistent with those statutory purposes.

B. Congress Did Not Authorize Immigration Enforcement Uses and Its Silence Is Dispositive

Congress considered these programs carefully, making deliberate decisions about who should receive assistance, the conditions that should apply, and the safeguards that should protect applicants. In every instance, Congress declined to build immigration enforcement hooks into the programs. The ERA programs, the Homeowner Assistance Fund, the State and Local Fiscal Recovery Funds—none of them include a provision authorizing the collection or use of beneficiary data for immigration enforcement purposes, and none make immigration status a basis for disqualification in the program's eligibility criteria.

Congressional silence on this point is deliberate. When Congress wants to build immigration enforcement mechanisms into federal benefit programs, it knows how to do so explicitly. It did not do so here. Treasury cannot accomplish through administrative action—through a system of records notice—what Congress expressly declined to authorize legislatively. Using program-specific data for purposes that fall outside the statutory purposes of the authorizing legislation is arbitrary, capricious, and contrary to law under 5 U.S.C. § 706(2)(A), independent of any Privacy Act analysis.

As the Supreme Court has held, an agency "has relied on factors which Congress has not intended it to consider" when it acts for purposes outside its statutory authorization. *Motor Vehicle Manufacturers Ass'n v. State Farm*, 463 U.S. 29, 43 (1983). The proposition that Treasury may consolidate emergency relief program data for immigration enforcement because no statute explicitly prohibits this is the argument that the APA arbitrary-and-capricious standard forecloses. An agency cannot simply do whatever is not forbidden. It must act within the purposes for which it was authorized to act.

C. Repurposing These Data Constitutes a Form of Data Betrayal

The concept of data betrayal applies with particular force to the statutory analysis. Each of the programs covered by this SORN was designed to reach vulnerable populations during moments of acute crisis. The Emergency Rental Assistance programs served the needs of families facing eviction. The Homeowner Assistance Fund supported homeowners facing foreclosure. The State Small Business Credit Initiative targeted assistance for small businesses—including many Latino-owned businesses—that could not access traditional capital markets.

The populations served by these programs are similar or adjacent to people who face the greatest risk from immigration enforcement repurposing of their data. Mixed-status families—families in which some members are citizens and others are undocumented—were among the primary beneficiaries of ERA and HAF in many states. They disclosed their household composition, income, and addresses in the context of programs that Congress designed to help them. The statutory purposes of those programs are violated when their data are repurposed against them.

This is the core of data betrayal in the statutory context: the government induced disclosure by offering a benefit, collected information under a statutory framework that defined a specific legitimate purpose, and now proposes to use that information for a purpose adverse to the people who disclosed it. Each program statute that authorized the original collection prohibits this repurposing. The Privacy Act's compatible-use requirement codifies that prohibition as a matter of administrative law.

D. Consolidation of State-Administered Program Data Raises Additional Federalism Concerns

Many programs covered by this notice were administered by states, localities, and tribal governments, which collected applicant data directly and made representations—explicit and implicit—to applicants about how their information would be used in a manner consistent with current law. For example, states that administered the ERA programs designed their intake processes, their eligibility forms, and their privacy notices around the program-specific purposes for which federal law authorized data collection. Similarly, applicants in mixed-status households disclosed sensitive personal and financial information specifically because program administrators represented that it would be used only to determine eligibility for housing assistance.

Treasury's proposed consolidation asserts federal control over data collected by state and local entities in ways that those entities did not contemplate and applicants did not consent to. This raises serious concerns under the Tenth Amendment's anti-commandeering doctrine. The federal government cannot compel states to administer federal programs and then treat the data those states collected in the course of administration as freely available federal property to be repurposed for federal enforcement objectives.

In *New York v. United States*, 505 U.S. 144 (1992), and *Printz v. United States*, 521 U.S. 898 (1997), the Supreme Court established that the federal government may not commandeer state governmental machinery for federal purposes. While those cases addressed direct commandeering of state executive officials, the underlying principle applies to data as well: states that administered these programs as partners in a cooperative federal-state framework did not surrender their residents' sensitive personal information to be repurposed for federal immigration enforcement. EO 14243's assertion of "unfettered access" to data from state programs that receive federal funding is a breathtaking claim of federal authority that exceeds any statutory authorization and that conflicts directly with the terms under which states collected these data.

States that administered the ERA, HAF, and SLFRF programs have their own interests in the integrity of the data collection process, their own legal obligations to their residents under state privacy laws, and their own relationships of trust with the communities they served. Treasury's proposed consolidation disregards all of these interests without explanation or statutory justification.

This serious federalism problem is compounded by Treasury's reliance, which is unacknowledged in the SORN, on grant audit authority as the mechanism for compelling data production. The most plausible legal basis for Treasury's data collection from grantees is 2 C.F.R. § 200.337, the Uniform Guidance provision giving federal agencies access to grantee records pertinent to a federal award.

But § 200.337 is not an unlimited right of access. It explicitly requires that agencies and their authorized representatives "take measures to protect the name of victims of a crime when access to the victim's name is necessary." And the provision goes further: "only under extraordinary and rare circumstances would such access include a review of the true name of victims of a crime," specifies that "routine monitoring cannot be considered extraordinary and rare circumstances," and provides that any such access outside of a court order or subpoena must be approved by the head or delegate of the federal agency.

The statute contemplates record access in the context of specific audits of specific awards, not the wholesale aggregation of beneficiary-level data from millions of individuals across dozens of programs into a centralized federal repository. States that administered these programs as cooperative federalism partners collected applicant data in reliance on and compliance with both federal program requirements and their own state privacy frameworks. They did not collect it as data entry agents for a federal enforcement database. Treasury's invocation of audit authority to accomplish wholesale data consolidation exceeds the scope of that authority and is independently contrary to law under 5 U.S.C. § 706(2)(C).

V. THE PROPOSED SYSTEM VIOLATES MULTIPLE SPECIFIC MANDATORY REQUIREMENTS OF THE PRIVACY ACT

The proposed system of records also violates five specific mandatory requirements of the Privacy Act, failing baseline procedural and substantive requirements at every level.

A. The Proposed Routine Uses Are Incompatible with Original Collection Purposes (5 U.S.C. § 552a(b)(3))

The Privacy Act's compatible-use requirement is the statute's central substantive protection. It provides that agencies may only disclose records as a "routine use" if the disclosure is "compatible with the purpose for which [the information] was collected." 5 U.S.C. § 552a(a)(7), (b)(3). OMB Circular A-108 (2016) requires agencies to explain how each proposed routine use satisfies this compatibility requirement. The original OMB Privacy Act Implementation Guidelines confirm that a routine use "must be not only compatible with, but related to, the purpose for which the record is maintained." OMB, Privacy Act Guidelines, 40 Fed. Reg. 28949, 28953 (July 1, 1975), https://perma.cc/776J-4L46. The compatible-use requirement prevents

"personal data collected by one organization for a stated purpose" from being "used and traded by another organization for a completely unrelated purpose," which could "seriously threaten[]" "individual rights." *Britt v. Naval* Investigative Serv., 886 F.2d 544, 549-50 (3d Cir. 1989) (quoting 120 Cong. Rec. 36,894 (1974) (statement of Sen. Percy)).

Data in these programs were collected to determine eligibility for housing and economic relief—specifically, to establish whether a family qualified for emergency rental assistance, whether a homeowner qualified for mortgage relief, whether a small business qualified for credit support.

The purpose was remedial, protective, and individual. Disclosing that data for "identification and prevention of fraud, waste, and abuse" across federal agencies—Routine Use (2) as proposed—is incompatible with that purpose. As drafted, Routine Use (2) is a blank check for disclosure to any federal agency claiming any fraud prevention purpose.

Using it for law enforcement referrals in connection with "potential violations of civil or criminal law"—Routine Use (4) as proposed—is incompatible with that purpose. Sharing it with immigration enforcement agencies is also incompatible with that purpose. These are fundamentally different kinds of governmental activity, involving fundamentally different legal relationships with the individuals whose data are at issue. Treasury made no showing of compatibility. It failed to analyze, program by program, how each proposed routine use relates to

the original collection purposes of each covered program. It did not engage with the OMB guidance that requires such analysis. This is legally insufficient. OMB Circular A-108 requires the analysis. The statute requires the compatibility.

Routine Use (2) is particularly problematic. As drafted, it authorizes disclosure to "Federal agencies, non-Federal entities, their employees, and agents" for "identification and prevention of fraud, waste, and abuse." This language tracks EO 14243's stated purpose directly and is written without meaningful limitation. There is no requirement that the receiving agency identify a specific program, a specific type of fraud, or a specific legal basis for the request.

The SORN's treatment of IRS-sourced data across its routine uses reveals an internal inconsistency. Routine Use 13 contains an explicit carve-out: "addresses obtained from the Internal Revenue Service shall not be disclosed to other agencies." This language acknowledges that IRS-sourced address data are subject to heightened statutory protection under 26 U.S.C. § 6103 and cannot be freely shared even with other federal agencies.

Yet Routine Uses 14 and 15 purport to authorize disclosure of IRS-sourced mailing addresses to private consumer reporting agencies (RU 14) and private debt collection agencies (RU 15)—disclosures that are also barred under federal law.

B. The SORN Violates the Notice-at-Collection Requirement (5 U.S.C. § 552a(e)(3))

The Privacy Act requires agencies to inform individuals at the time of collection of the authority for collection, the principal purpose for which the information is to be used, the routine uses that may be made of it, and the consequences of not providing the requested information. 5 U.S.C. § 552a(e)(3). This requirement exists to enable individuals to make informed decisions

about whether to disclose sensitive personal information to the government, and to hold the government accountable to the representations it made when it sought that information.

The Privacy Act's public notice and comment structure is an essential component of the Act and an essential piece of American democracy. Americans deserve to know the nature, scope, and routine uses of the records before they are collected by the federal government. Millions of applicants for the Emergency Rental Assistance programs, the Homeowner Assistance Fund, the State Small Business Credit Initiative, and the other programs covered by this SORN received no notice at the time of collection that their data could be consolidated into a cross-agency federal database, shared with law enforcement agencies for potential civil or criminal violations, or made available for the purposes described in the proposed routine uses. They were told, instead, that their information would be used to determine their eligibility for the specific relief program they were applying to. That is the representation on which they relied when they disclosed their Social Security numbers, their household incomes, their family compositions, and their addresses.

The proposed system retroactively transforms that disclosure into something it was never represented to be: a contribution to a federal database subject to broad enforcement uses. The government cannot obtain sensitive personal information under representations about its limited use, then expand those uses without the knowledge or consent of the people who disclosed it. The notice-at-collection requirement exists precisely to prevent this.

C. The SORN Fails the Specificity Requirement (5 U.S.C. § 552a(e)(4)(D))

The Privacy Act requires that SORNs include "each routine use of the records contained in the system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D). Routine use descriptions must be sufficiently specific to allow an individual to make an informed judgment about whether to provide personal information to an agency. A routine use that covers essentially all possible disclosure scenarios under an opaque label of "fraud, waste, and abuse" or "civil or criminal law violation" does not satisfy this standard.

As OMB Circular A-108 makes clear, "[r]outine uses shall be narrowly tailored to address a specific and appropriate use of the records," and "[a]gencies shall describe each routine use with sufficient clarity and specificity to ensure that members of the public who are unfamiliar with the system or the agency's program can understand the uses to which the records are subject." OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act. The Circular further provides that "[o]verly broad or ambiguous language would undermine the purpose of the routine use notice requirement and shall be avoided." *Id.*

From reading the proposed routine uses, an individual cannot determine: whether their information might be shared with DHS or ICE; whether it might be shared with state election officials for voter verification purposes; whether it might be shared with local law enforcement agencies; whether it might be shared with federal prosecutors; or for what specific purpose any such sharing might occur. The categories of users and purposes are defined at such a level of generality that they provide no meaningful information. The vagueness appears to be an attempt

to preserve maximum administrative discretion to share data for purposes that could not survive scrutiny if stated explicitly.

The specificity requirement serves an accountability function. An agency that commits in its SORN to sharing data only in defined circumstances can be held accountable to those commitments. An agency that defines its routine uses with sufficient vagueness to cover any conceivable disclosure cannot be held accountable to anything. The proposed routine uses fail the specificity requirement.

Additionally, Routine Use 5 permits disclosure to any public authority for purposes of hiring, security clearance, licensing, or grant decisions, "or other benefit," with no requirement of an individualized request or prior written consent from the subject. The Privacy Act contemplates that routine uses are appropriate only where prior written consent is impracticable. For employment, security clearance, and professional licensure decisions, prior written consent from the applicant is not only practicable, it is the standard practice and appropriate mechanism.

Using a routine use to bypass consent in these contexts is impermissible. As drafted, Routine Use 5 would permit Treasury to disclose records about every individual in this system to every state licensing board for any conceivable future employment or licensing decision, in bulk, without any individualized request and without the subject's knowledge. The phrase "or other benefit" included at the end of the routine use extends this further still, potentially encompassing state voter registration processes, public housing applications, or any other governmental benefit program. This is not a routine use. It is an unlimited background check service and invitation to unlawful and arbitrary action by the state.

Routine Use 10, permitting disclosure to "a public or professional licensing organization" when Treasury's records indicate "a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual," is entirely untethered from the purposes for which any of the covered programs authorized data collection.

Treasury collected these data—or rather, states and localities collected it, under program-specific statutory frameworks—to determine eligibility for housing and economic relief. None of those frameworks authorize Treasury to operate a multi-state professional licensing surveillance system. The populations covered by this system include sole proprietors, small business owners, and community members who disclosed sensitive personal and financial information in the context of benefit applications. Repurposing that data to initiate or support professional licensing proceedings against them without individualized notice, without a specific pending investigation by the licensing body, and based on information they never consented to share for that purpose fails the compatibility requirement, the notice-at-collection requirement, and the specificity requirement all.

Routine Uses 6 and 12 both address litigation-related disclosures, and both suffer from an overbreadth that the D.C. Circuit has specifically identified as impermissible. As drafted, Routine Use 6 authorizes disclosure "in a proceeding before a court, adjudicative body, or other administrative body," language broad enough to encompass disclosure in response to administrative subpoenas and civil discovery requests.

In *Doe v. DiGenova*, 779 F.2d 74 (D.C. Cir. 1985), the D.C. Circuit held that a subpoena is not a court order within the meaning of 5 U.S.C. § 552a(b)(11). The court further held in *Doe v. Stephens*, 851 F.2d 1457, 1465–67 (D.C. Cir. 1988), that an agency may not release Privacy Act-protected records in response to a subpoena by relying on a routine use. Agencies cannot use routine uses to circumvent the limitations Congress built into the court order exception. A discovery request carries even less process than a subpoena; a subpoena at least issues in the name of the court, while a discovery request is merely party-initiated. If a subpoena does not satisfy § 552a(b)(11), neither does a discovery request.

The appropriate mechanism for handling Privacy Act records in litigation—a negotiated stipulation incorporating a protective order, signed by the presiding judge—is not described in either routine use. Routine Use 12 partially duplicates Routine Use 6 while adding explicit reference to "disclosures to opposing counsel or witnesses in the course of civil discovery," which, read literally, would authorize the government to hand these records to private opposing counsel in any litigation where Treasury has an interest. None of this is what the Privacy Act's litigation disclosure provisions contemplate, and the routine use language does not satisfy the specificity requirement.

D. The SORN Fails the Accuracy Requirement (5 U.S.C. § 552a(e)(5))

The Privacy Act requires agencies to maintain records used in making determinations about individuals "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C. § 552a(e)(5). This requirement is not merely aspirational. It is a mandatory condition that must be satisfied before records may be used to make adverse determinations affecting individuals.

The data collected under the programs covered by this SORN were collected under emergency conditions, often with relaxed verification standards, over a period of several years. Much of it is now years old. Household compositions change. Income levels change. People move. The data that were accurate for purposes of determining emergency rental assistance eligibility in 2021 or 2022 may bear little relationship to current household circumstances. Treasury has made no showing that these data are accurate, relevant, timely, or complete for the proposed new enforcement uses.

The consequences of using inaccurate data for enforcement purposes are not theoretical. The IRS-ICE data sharing experience provides a precise and instructive illustration: when ICE submitted a mass request for the addresses of 1.28 million taxpayers, the IRS was able to confirm only approximately 47,000 records—a 97% failure rate. Families whose outdated information appears in these systems face the prospect of enforcement actions based on records that no longer accurately reflect their circumstances. The accuracy requirement exists to prevent exactly this outcome. Treasury has not demonstrated compliance with it, and no showing has been made that the consolidated system would satisfy this standard for any of the proposed enforcement uses.

E. The SORN Fails to Establish Adequate Security Safeguards (5 U.S.C. § 552a(e)(9), (e)(10); FISMA)

The Privacy Act requires agencies to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records" and to prevent "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. § 552a(e)(10). Agencies must also establish rules of conduct for personnel operating the system and train them in the requirements of the Act. 5 U.S.C. § 552a(e)(9). FISMA reinforces these requirements, mandating that agencies implement security controls "commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction" of the information. 44 U.S.C. § 3554(a)(1).

A consolidated system containing sensitive personal and financial data from eight separate programs covering millions of Americans presents materially greater security risks than the separate program-specific systems from which the data would be drawn. The attack surface is larger. The potential damage from a breach is greater. The number of individuals whose data would be compromised in a single incident is higher. Treasury has provided no security assessment of the proposed consolidated system, no analysis of the incremental security risks created by consolidation, and no description of security controls adequate to the risk profile of the proposed system.

This is not a minor gap. The documentation of security incidents at Treasury and related agencies during 2025—including DOGE-related access to Treasury systems and the erroneous disclosure of 47,000 taxpayer records to ICE—demonstrates that these are not hypothetical risks. Treasury has a documented record of security failures in the very period during which this SORN was being developed. It cannot satisfy the security safeguards requirement of the Privacy Act or FISMA by asserting, in boilerplate language, that "records are safeguarded in accordance with applicable laws and policies." The law requires more.

The security safeguards failure is further illustrated by Routine Use 18, which would permit disclosure to "a student participating in a Treasury student volunteer program, where such disclosure is necessary to support program functions of Treasury." This routine use has no place in a system containing the sensitive personal and financial records of millions of benefit program applicants, including Social Security numbers, taxpayer identification numbers, household income data, and family composition information for mixed-status households. Student volunteers are not federal employees. They are not subject to the same background check requirements, security training obligations, or civil and criminal penalties for unauthorized disclosure. Permitting their access to records of this sensitivity and scale fails the security safeguards requirement of 5 U.S.C. § 552a(e)(9) and (e)(10) and is incompatible with the Privacy Act's requirement that agencies limit access to those with a demonstrated need. If this a *post hoc* attempt to legalize DOGE access, it fails on its face.

The SORN fails to specify which National Archives and Records Administration (NARA) records retention schedules govern this system. Retention schedules are the mechanism by which records that have served their authorized purpose are identified for timely disposal, limiting the

period during which sensitive personal data are at risk of breach, unauthorized access, or incompatible use.

For a newly consolidated system drawing on records from eight distinct programs—each of which may be subject to a different existing NARA schedule, or none—Treasury must identify which schedules apply and, where no approved schedule exists, affirmatively state that the records will be treated as permanently valuable until a schedule is approved. The absence of a retention framework means that sensitive personal and financial data collected during the COVID-19 pandemic emergency could remain in an active, accessible consolidated federal system indefinitely, subject to the broad routine uses proposed here, with no legal mechanism compelling its disposal. This is inconsistent with the Privacy Act's data minimization principles and FISMA's requirement that security controls be commensurate with the ongoing risk profile of maintained records.

F. A Computer Matching Agreement Is Required (5 U.S.C. § 552a(o))

The Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503, 5 U.S.C. § 552a(o), requires that when agencies engage in automated comparison of records from two or more federal systems of records—or from a federal system and non-federal records—they must execute written Computer Matching Agreements containing specific safeguards, obtain Data Integrity Board review, and include cost-benefit analysis demonstrating the program is "likely to be cost effective." These requirements exist because Congress recognized that automated cross-system data matching poses unique privacy risks requiring specific procedural protections.

These procedural safeguards extend to matching programs as well. Notice of any matching program with a non-Federal agency must be published in the Federal Register "at least 30 days prior to conducting such program." 5 U.S.C. § 552a(e)(12). This advance notice requirement ensures that the public has a meaningful opportunity to learn about and respond to proposed data-sharing arrangements before they take effect.

OMB guidelines reinforce this obligation, requiring agencies to review and consider any "public comments on a . . . published matching [program] notice." OMB Circular A-108 at 7, 19; 40 Fed. Reg. at 28,966. Together, these provisions reflect Congress's determination that the comparison and cross-referencing of government records, with its heightened potential for harm to individuals, demands advance public scrutiny, not post hoc ratification.

The routine uses proposed in this SORN, including disclosure to federal agencies for fraud detection, law enforcement referrals, and statistical analysis, plainly contemplate automated cross-referencing of beneficiary records across programs and against other federal datasets. This is the definition of computer matching. If Treasury intends to use this consolidated system for any automated cross-referencing of records—and the routine uses strongly suggest it does—a Computer Matching Agreement is a legal prerequisite. No such agreement has been published. This is an independent and sufficient basis for withdrawal of this notice.

VI. THE PROPOSED SYSTEM CONFLICTS WITH SECTION 6103 OF THE INTERNAL REVENUE CODE AND RECENT FEDERAL COURT DECISIONS

A. Section 6103's Strict Confidentiality Framework

Section 6103 of the Internal Revenue Code, 26 U.S.C. § 6103, establishes one of the most comprehensive confidentiality regimes in federal law. Subsection (a) commands, without qualification, that "returns and return information shall be confidential." The statute defines "return information" broadly to encompass not only tax returns themselves but "any other data received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability." 26 U.S.C. § 6103(b)(2). This definition includes the income documentation, financial records, and tax transcripts that applicants for the programs covered by this SORN submitted as eligibility verification.

Section 6103 was enacted in the Tax Reform Act of 1976, in direct response to the Nixon administration's use of IRS data to target political opponents. Congress's purpose was unambiguous: to create an ironclad statutory barrier against the use of tax-related financial information for purposes other than tax administration, enforceable against the executive branch regardless of presidential preference. As the D.C. Circuit explained in *Gardner v. United States*, 213 F.3d 735, 738 (D.C. Cir. 2000), § 6103 "guarantees that the sometimes sensitive or otherwise personal information in a return will be guarded from persons not directly engaged in processing or inspecting the return for tax administration purposes." The statute reflects a fundamental compact: Americans are required by law to disclose their financial circumstances to the federal government for tax purposes, and the government is required by law to hold that information in strict confidence.

The exceptions to § 6103's confidentiality mandate are narrow and specific. Section 6103(h)(1) allows Treasury employees to access return information only for "tax administration purposes." Section 6103(i)(2) permits disclosure to federal law enforcement, but only on a case-by-case basis, only for specific officers "personally and directly engaged" in a specific criminal investigation, and only for information that may be relevant to that specific investigation. There is no general exception for civil immigration enforcement, no exception for bulk data requests, and no exception for cross-agency consolidation programs directed by Executive Order. As explained above, data sharing by IRS is also currently enjoined.

B. The Programs Covered by This SORN Collected Tax-Related Financial Information Subject to § 6103

Treasury's proposed SORN is not limited to data that are entirely separate from the § 6103 framework. The financial assistance programs covered by this notice—particularly the Emergency Rental Assistance programs and the Homeowner Assistance Fund—require applicants to submit income documentation that was verified against IRS records, to provide tax return transcripts, and to furnish Social Security numbers and Individual Taxpayer Identification Numbers that are identifiers in the IRS's return information system.

Under the broad definition of "return information" in 26 U.S.C. § 6103(b)(2), much of the financial eligibility data collected in connection with these programs constitutes return

information subject to § 6103's confidentiality protections. It was derived from or cross-referenced against IRS records. It was collected by Treasury's own systems or by state agencies operating under Treasury's oversight. It was also submitted by individuals who understood it would be treated with the confidentiality that tax-related financial information commands.

Treasury cannot evade this analysis by characterizing the data as "program administration" information rather than "tax" information. Further, the statutory definition of return information is not limited to information formally submitted on a tax return. It includes any data received, recorded, or collected in connection with determining tax liability, including the income and financial data submitted to verify eligibility for programs in which the eligibility criteria are defined by reference to income thresholds drawn from tax return data. The § 6103 framework applies to much of what this SORN proposes to consolidate and share.

C. Multiple Injunctions Currently Bar Sharing of Tax Data

In *Community Economic Development Center of Southeastern Massachusetts et al. v. Bessent et al.*, U.S. District Court for the District of Massachusetts (Feb. 5, 2026), Judge Indira Talwani issued a preliminary injunction finding that the administration's sharing of taxpayer address data with ICE likely violated § 6103. The court found that plaintiffs demonstrated a "high likelihood" that ICE's handling of taxpayer addresses "violated and continues to violate" the Internal Revenue Code. Section 6103, the court held, "strictly prohibits the disclosure" of taxpayer data to government agencies for purposes outside those Congress specifically authorized.

The Massachusetts court's reasoning applies with full force to Treasury's proposed system. The court found that the government's sharing of IRS-held financial data with immigration enforcement agencies was not covered by any of § 6103's enumerated exceptions—not the tax administration exception, not the law enforcement exception (which requires case-by-case specificity and a nexus to a particular criminal investigation), and not any other provision.

The court also found that the irreparable harm from such data sharing includes the "erosion of community trust" that occurs when government agencies repurpose tax-related financial information for immigration enforcement.

In *Center for Taxpayer Rights et al. v. Internal Revenue Service et al.*, No. 1:25-cv-00457 (D.D.C.), Judge Colleen Kollar-Kotelly issued a parallel injunction blocking IRS disclosure of taxpayer address data to DHS and ICE. The court found the administration's "Address-Sharing Policy" to be unlawful under § 6103 and arbitrary and capricious under the APA. That decision further established that the § 6103(i)(2) law enforcement exception does not authorize mass bulk requests—a point developed extensively in briefing in *Centro de Trabajadores Unidos v. Bessent*, No. 1:25-cv-00677 (D.D.C.), a related proceeding before the federal district.

The § 6103 problem is not confined to the general analytical framework. It surfaces directly in this SORN's own text, as described above with respect to Routine Uses 13 through 15. Treasury cannot on one hand acknowledge § 6103's bar on inter-agency IRS address sharing and on the other hand authorize disclosure of the same addresses to private commercial entities. This

internal inconsistency further confirms that the § 6103 framework has not been applied consistently or rigorously to the routine uses in this notice.

D. Unlawful Sharing of Tax Records Violates Public Trust

In *Center for Taxpayer Rights v. IRS*, the court held that § 6103 creates a "relationship of trust" between the government and the individuals who disclose financial information under legal compulsion, and that the harm from violating that relationship "occurs when the plaintiff's trust in the breaching party is violated, whether or not the breach has other consequences." This violation of the trust relationship is itself cognizable injury, independent of any downstream deportation, audit, enforcement action, or other harm.

The same analysis applies to the data collected under the financial assistance programs covered by this SORN. The individuals who applied for emergency rental assistance, homeowner relief, and small business credit programs disclosed sensitive personal and financial information in a context defined by an implicit and often explicit compact: provide this information, and it will be used to determine your eligibility for this program. The government induced that disclosure. It benefited from it in that it could not have administered the programs without it. And it is now proposing, without statutory authority, to repurpose that information in ways that are adverse to the people who provided it.

Section 6103's confidentiality framework, the Privacy Act's compatible-use requirement, and the program statutes' specific authorizations all reflect the same underlying principle: when the government induces individuals to disclose sensitive information for a defined and limited purpose, it must honor the terms of that disclosure.

VII. THE PROPOSED SYSTEM CAUSES CONCRETE AND FORESEEABLE HARM TO LATINO AND MIXED-STATUS FAMILIES

The harm from this proposed system is not speculative. It falls predictably and with particular severity on Latino families—the communities UnidosUS was founded to serve and has represented for more than 55 years. Latino families are disproportionately represented among the beneficiaries of the Emergency Rental Assistance programs, the Homeowner Assistance Fund, and the State Small Business Credit Initiative, both because Latino workers and small business owners were disproportionately affected by the economic disruptions of the COVID-19 pandemic and because UnidosUS and its nearly 300 affiliated organizations invested significant resources in ensuring that Latino families could access the relief Congress intended them to receive.

A substantial portion of the Latino families served by these programs are mixed-status households: families in which some members are U.S. citizens, some are lawful permanent residents, and some are undocumented. These are not rare or marginal cases. They are a defining feature of the Latino community in the United States, where decades of failed immigration policy have created millions of families whose members hold different legal statuses. Mixed-status families made careful and often agonizing decisions about whether to seek government assistance during the pandemic, weighing their urgent need for help against their fear of

exposure. Many disclosed their household composition, their ITINs, and their family members' immigration-adjacent information specifically because program administrators and trusted community organizations told them it was safe to do so—that the data would be protected and used only to determine their eligibility for the program. That assurance is what this SORN proposes to revoke, retroactively and without their consent.

The Privacy Act, the underlying program statutes, and longstanding agency practice together create a relationship of trust between the government and the individuals who disclose sensitive personal and financial information to qualify for federal benefit programs. That relationship is violated the moment the government repurposes the information for a purpose incompatible with the purpose under which it was collected, regardless of whether any specific individual is thereafter subjected to an enforcement action. The harm is not future and speculative, but rather immediate, legally cognizable and structural in nature.

Treasury is proposing to violate a relationship of trust with millions of people who had no meaningful choice about whether to disclose their information. The power asymmetry between a family facing eviction and the government agency offering to prevent that eviction is total. The family discloses or it loses its home. The government's commitment to use that disclosure only for the stated purpose is not a courtesy, it is the condition on which the entire transactional legitimacy of the benefit program rests. To repurpose the disclosure is to invalidate that transaction retroactively and to expose the original offer of assistance as a mechanism for obtaining adverse information under false pretenses.

The proposed system also creates foreseeable and severe downstream harms for the individuals whose data would be consolidated and shared. Families who received lawful housing assistance face deportation risk based on data they disclosed in good faith. An undocumented family member whose ITIN appears in an ERA application file—disclosed for the purpose of proving household income and establishing eligibility for rent relief—becomes identifiable and locatable for immigration enforcement purposes the moment that data enters a system with routine uses that contemplate disclosure to federal law enforcement. The family member did not consent to this use, nor does the program statute authorize this use.

The accuracy problem compounds the harm. As documented in the IRS-ICE context, the data collected under these programs contains significant error rates, including outdated addresses, mismatched identifiers, and records reflecting household compositions that have since changed. A 97% error rate on a mass data request, as documented in the IRS-ICE matter, means that enforcement actions predicated on this data will predominantly fall on people who have no relationship to the records used to identify them. For immigration enforcement purposes, that means citizens, lawful permanent residents, and individuals whose immigration status has changed since the data was collected will face disproportionate enforcement exposure based on records that do not accurately reflect their current circumstances.

The damage to community trust extends far beyond the individuals whose data are misused. The Latino community's willingness to engage with federal assistance programs, to disclose personal and financial information to government agencies, and to participate in the federal benefit system

depends on confidence that the government will honor its commitments about how that information will be used.

The IRS-ICE data sharing debacle has already caused documented chilling effects on tax filing in immigrant communities: people who are legally required to file tax returns are not filing them because they fear their information will be used against them. Kevin G. Andrade, *Many Immigrants Have Stopped Filing Taxes out of Fear*, New Bedford Light (Feb. 2026), https://newbedfordlight.org/many-immigrants-have-stopped-filing-taxes-out-of-fear/. Treasury's proposed consolidation of financial assistance program data will produce the same chilling effects on participation in benefit programs that Congress designed specifically to reach vulnerable populations.

There is also a practical dimension to the Paperwork Reduction Act (PRA) that deserves particular attention in this context. Under the PRA's public protection clause, 44 U.S.C. § 3512, no person is required to respond to a collection of information that has not been approved by OMB and does not display a valid OMB Control Number. This protection extends to state and local governments, which are "persons" for purposes of the PRA.

States and localities that administered the programs covered by this SORN collected beneficiary data under program-specific frameworks with specific statutory purposes. They are not obligated to transmit that data to Treasury in response to requests that have not been cleared through the OMB PRA process. Community organizations, housing advocates, and legal services providers working with affected families should be aware that states have a right to decline compliance with uncleaned data requests, and that Treasury's failure to obtain OMB clearance for the data collection is a legally enforceable defect that affected parties can raise.

The Massachusetts and D.C. federal courts that enjoined this data sharing found irreparable harm not only to the specific individuals whose data was disclosed but to the entire community of taxpayers who rely on the confidentiality of the tax system. As the court found in *Community Economic Development Center of Southeastern Massachusetts et al. v. Bessent et al.*, erosion of community trust from repurposing tax-related data for immigration enforcement is itself irreparable harm—harm that cannot be undone once the disclosure occurs and harm that spreads through communities even when individual data points are later corrected or expunged. Treasury is proposing to replicate this harm across a different but equally sensitive domain: the financial assistance program data of millions of families who sought help during one of the most acute economic crises in modern American history.

E. The Harm to Democratic Participation and Institutional Trust

The harms from this proposed system extend beyond the individuals whose data would be affected. They extend to the integrity of the federal benefit system itself and to the democratic compact between government and governed.

Federal assistance programs work because people trust them. The Emergency Rental Assistance program reached millions of families because housing advocates, community organizations, and trusted intermediaries like UnidosUS affiliates could tell vulnerable families that the program

was safe to access. If Treasury's proposed consolidation is implemented, that assurance will no longer be credible. Every future federal benefit program that serves immigrant communities, mixed-status families, or any population with reason to fear government surveillance will face a structural credibility deficit. The government will have demonstrated, through this SORN, that data collected in the context of benefit programs can be and will be repurposed for enforcement, regardless of statutory constraints.

This is not a consequence that can be repaired after the fact. Once the government has demonstrated that it treats benefit program data as a potential enforcement resource, the communities who need those benefits most will decline to access them. That means Congress's relief programs will not reach the people they were designed to reach. It means the economic and social purposes those programs serve will be undermined. And it means the implicit promise at the heart of every government benefit program—that the government is offering help, not gathering intelligence—will have been broken in a way that no subsequent assurance can repair. UnidosUS and its affiliates have spent decades building the trust that allows Latino families to engage with government programs. This SORN proposes to destroy that trust.

IX. REQUESTED ACTIONS

For the reasons set forth in these comments, UnidosUS and CREW demand that the Department of the Treasury take the following actions:

1. Withdraw this notice immediately. The proposed system of records must be withdrawn in its entirety. It is legally deficient under the Privacy Act, the APA, Section 6103 of the Internal Revenue Code, FISMA, and the underlying program statutes. The proposal to consolidate sensitive personal and financial data from eight distinct congressional programs into a single system of records with broad cross-agency disclosure authorities is not a valid administrative notice. It is an abuse of the SORN process to accomplish data consolidation for enforcement purposes that Congress has not authorized.

2. Immediately cease any cross-program data consolidation already underway. Treasury has not disclosed whether the consolidation described in this SORN has already begun under the authority of EO 14243 or otherwise. If any such consolidation is already in progress, it is a clear and ongoing Privacy Act violation not curable by a retroactive administrative notice. Treasury must immediately disclose the full timeline of any cross-program data access or consolidation activity, including any access by DOGE-affiliated personnel or contractors, and must immediately cease any such activity pending lawful authorization that does not currently exist.

3. Acknowledge the legal limits of Executive Order 14243 as a legal authority. An executive order cannot override mandatory statutory prohibitions. Treasury must acknowledge and affirm that EO 14243 does not and cannot authorize disclosures that the Privacy Act, Section 6103, or the underlying program statutes prohibit. The administration's theory that executive authority to manage federal records includes authority to repurpose them for any purpose the executive finds convenient is not a valid legal theory. It has been twice rejected by federal courts in the IRS-ICE context, and it is equally invalid here. Treasury's reliance on EO 14243 as legal authority confirms that the aim of this system is data betrayal, not program administration.

4. Decline to reissue any version of this proposal absent affirmative Congressional authorization. The fundamental defect of the proposed system is not procedural. It is that Congress has not authorized the consolidation of these separately enacted programs' data into a unified enforcement-adjacent database. That authorization cannot be supplied by an executive order, a SORN, or a rulemaking. It requires an act of Congress. Until Congress explicitly authorizes the consolidation of these programs' data and the routine uses Treasury is seeking to establish, no legally compliant version of this proposal is possible. We urge Treasury to acknowledge this constraint rather than attempting to achieve through administrative creativity what statutory law does not permit.

5. Commit affirmatively that no data from these programs will be shared with immigration enforcement agencies. The evident purpose of this SORN—confirmed by the citation of EO 14243, the breadth of proposed Routine Use (2), and the context of the administration's broader data consolidation agenda—is to make financial assistance program data available for immigration enforcement. Treasury must publicly and explicitly commit that no data collected under the Emergency Rental Assistance programs, the Homeowner Assistance Fund, the State and Local Fiscal Recovery Funds, the State Small Business Credit Initiative, or any other program covered by this SORN will be shared with the Department of Homeland Security, Immigration and Customs Enforcement, U.S. Customs and Border Protection, or any other immigration enforcement agency, for any purpose. That commitment must be backed by enforceable legal mechanisms, not administrative assurances.

6. Extend the comment period to no fewer than 60 days and provide complete disclosure of all DOGE-related data access. The current 30-day comment period is inadequate for a proposal of this legal complexity and magnitude. Moreover, the public cannot meaningfully comment on a proposed system of records without understanding the full scope of data access that has already occurred under EO 14243 and related DOGE activities at Treasury. Treasury must disclose all instances of cross-program data access or sharing that have occurred since January 20, 2025, and must provide that disclosure before any revised comment period begins. The comment clock should not run until the public has the information it needs to comment meaningfully.

7. Obtain Paperwork Reduction Act clearance before conducting any data collection from grantees. The collection of beneficiary-level information from states, localities, and other grantees across eight programs covering millions of individuals constitutes a collection of information from a class of entities subject to PRA requirements. Treasury must obtain OMB review, publish the required Federal Register notices, and receive an assigned OMB Control Number before conducting or requiring any such collection. If any collection has already occurred without OMB clearance, Treasury must notify OMB and this Committee of the unauthorized collection as required by 44 U.S.C. § 3512, disclose the full scope of data already collected, and implement measures to prevent further collection until lawful clearance is obtained.

8. Demonstrate compliance with the ERA's domestic violence victim protections. Any revised notice must specifically address the mandatory privacy protections for domestic violence, sexual assault, and stalking victims established in 15 U.S.C. § 9058a(4) and demonstrate that no ERA data relating to such victims will be accessible through any of the proposed routine uses,

including the law enforcement referral and fraud prevention uses in Routine Uses 2 and 4. Treasury must describe the technical and administrative mechanisms it will use to identify and segregate domestic violence victim data before any system operation begins.

IX. CONCLUSION

The Privacy Act of 1974 was born from a specific historical lesson: that the federal government's capacity to collect and centralize personal information, if left unchecked, can be turned against the people from whom that information was taken. Congress enacted the Act after the Nixon administration used IRS data to target political opponents and COINTELPRO used federal records to surveil and harass civil rights leaders. The Act's core commands—that data collected for one purpose may not be used for another, that individuals must be informed of the uses their data will serve, that centralized federal data banks are prohibited—were not technicalities but central, anchoring features of the statute.

Treasury's proposed system of records fails each of those commands. It proposes to consolidate data from eight separately authorized congressional programs—data collected from millions of families during moments of acute economic crisis, in reliance on the government's representations that it would be used to help them—into a single unified repository with broad cross-agency disclosure authorities. It cites as legal authority an executive order that cannot override multiple statutory requirements and constraints. Alarmingly, the SORN conflicts directly with Section 6103 of the Internal Revenue Code and the reasoning of two federal courts that have recently enjoined analogous data sharing. And its evident purpose—confirmed by the citation of EO 14243 and the breadth of its proposed routine uses—is to make financial assistance program data available for immigration enforcement against the communities who were most in need of that assistance.

This is, in its essence, an act of data betrayal: the weaponization of the apparatus of care against the people it was designed to serve. The families who disclosed their household compositions, their incomes, their addresses, and their family members' identifying information to qualify for emergency rental assistance or homeowner relief were not contributing to a federal enforcement database. They were asking for help. The government offered to help them—and collected detailed personal and financial information as the condition of that help—under an implicit and often explicit compact that the information would be used only for the stated purpose. Treasury now proposes to break that compact, without statutory authority, through an administrative notice that most of those families will never see.

UnidosUS calls on Treasury to withdraw this notice immediately and completely, and immediately cease any cross-program data consolidation already underway. We also call on Treasury to recognize, as Congress recognized fifty years ago, that the government's power to collect information from its citizens in the context of programs designed to serve them is a power held in trust, and is a trust that must be honored, not betrayed.