

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

U.S. DEPARTMENT OF AGRICULTURE

System of Records Notice, USDA/FNS-15: National Supplemental
Nutrition Assistance Program (SNAP) Information Database

90 Fed. Reg. 26,521 | FNS-2025-0024

July 16, 2025

The Electronic Privacy Information Center (EPIC) submits these comments in response to the System of Records Notice for USDA/FNS-15: “National Supplemental Nutrition Assistance Program (SNAP) Information Database,” published in the Federal Register by the U.S. Department of Agriculture (USDA) on June 23, 2025.¹ EPIC is a public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.

The proposed National SNAP Information Database (NSID) arises from USDA’s ongoing efforts to amass the sensitive personal information of tens of millions of SNAP recipients and applicants held by 53 state agencies into a single national database. USDA has claimed that such an unprecedented consolidation of personal data is necessary to eliminate “fraud” and “bureaucratic duplication and inefficiency”²—even though establishing such a database would create a singularly

¹ Privacy Act of 1974; System of Records, 90 Fed. Reg. 26,521.

² *FNS Data Sharing Guidance*, U.S. Dep’t of Agric. at 1 (May 6, 2025), <https://www.fns.usda.gov/sites/default/files/resource-files/fns-data-sharing-guidance5.6-V6-050625.pdf>.

rich target for hackers and fraudsters and duplicate the functions of the Congressionally-established (and far more secure) National Accuracy Clearinghouse.³ USDA has already been forced to suspend this data demand once before, owing to the agency’s failure to disclose key information required by the Privacy Act of 1974 and the Paperwork Reduction Act of 1980 and to solicit public comment thereon.⁴ USDA now seeks to cure that failure, in part, by publishing a System of Records Notice (Notice) for a proposed system that would house the sensitive personal data of every SNAP recipient and applicant in the country—data for which USDA recently renewed its demand.⁵

As set out below, the USDA’s efforts are unavailing. The System of Records Notice for the proposed NSID exhibits significant errors and omissions; provides for “routine uses” of SNAP data that are incompatible with both the purposes for which it was collected and express Title 7 protections for such data; and reveals numerous other violations of the Privacy Act that threaten to subject SNAP recipients and applicants to significant harm. USDA should withdraw its Notice, abandon its proposal to establish the NSID, and halt its unlawful efforts to compel states and EBT vendors to turn over the confidential personal data of SNAP recipients and applicants.

I. The Notice exhibits significant errors and omissions.

To begin with, USDA’s Notice misstates or fails to include certain key information, a reflection of the haste with which USDA has developed the proposed NSID. For example, the Notice misidentifies the instant proceeding as a “rulemaking” and omits basic information for email and mail submission of comments, leaving “[Insert email contact]” and “[Insert mail contact]”

³ *SNAP National Accuracy Clearinghouse (NAC)*, USDA (June 18, 2025), <https://www.fns.usda.gov/snap/nac>.

⁴ Zach Montague, *Trump Administration Backs Off Effort to Collect Data on Food Stamp Recipients*, N.Y. Times (June 3, 2025), <https://www.nytimes.com/2025/06/03/us/politics/trump-administration-personal-data-food-stamp-recipients.html>; see also *Pallek v. Rollins*, EPIC (June 2025), <https://epic.org/documents/pallek-v-rollins/>.

⁵ U.S. Dep’t of Agric., *SNAP Database -Letter to State Agencies* (July 9, 2025), <https://www.fns.usda.gov/snap/admin/database-letter>.

placeholders in the published version.⁶ The Notice also acknowledges that the NSID would be “maintained in the FNS Amazon Web Service (AWS) cloud infrastructure environment,” yet only lists address information for Microsoft as the “third-party service provider.”⁷ Either USDA has failed to disclose Microsoft’s role in the operation of the proposed NSID or has mistakenly used Microsoft’s address information in lieu of Amazon’s; either way, the Notice is clearly deficient.

More alarmingly, the Notice fails to identify any “polic[y or] practice[] of the agency regarding . . . disposal of the records,”⁸ proposing instead that “[a]ll records in this system will be kept indefinitely unless otherwise required by law until NARA has approved a records schedule for this system.”⁹ The suggestion that SNAP data might be kept “indefinitely”—that is, *never* disposed of—is precisely the opposite of a records disposal policy. USDA’s approach would expose SNAP recipients and applicants to a heightened risk of data breach and data misuse far beyond any colorable operational need for their personal information. Both the Privacy Act and the Code of Fair Information Practices obligate USDA to give adequate public notice of its disposal policies and practices, a requirement which cannot be satisfied by relying on a NARA records retention schedule that does not yet exist.¹⁰

⁶ 90 Fed. Reg. 26,521.

⁷ *Id.*

⁸ 5 U.S.C. § 552a(E)(4)(e).

⁹ 90 Fed. Reg. 26,523.

¹⁰ See 5 U.S.C. §§ 552a(e)(4)(E), (e)(11); Advisory Comm. on Automated Pers. Data Sys., U.S. Dep’t of Health, Educ., & Welfare, *Records, Computers and the Rights of Citizens* (1973), <https://www.justice.gov/opcl/docs/rec-com-rights.pdf> (“Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify: . . . The organization’s policies and practices regarding data storage, duration of retention of data, and disposal thereof[.]”).

II. The Notice proposes ‘routine uses’ for SNAP data that are incompatible with both the original purpose of collection and Title 7 protections for such data.

Although USDA seeks to grant itself tremendous latitude to use SNAP data contained in the NSID, several of the so-called “routine uses” set out in the Notice are not “compatible with the purpose for which [the SNAP data] was collected,”¹¹ and are therefore unlawful.

Because states certify SNAP eligibility and issue SNAP benefits, they have an operational need to collect and retain sensitive personal data on applicants and recipients. This includes an individual’s Social Security number, date of birth, address, employment status, citizenship status, income, resources, and more.¹² The purposes for which this data may be disclosed are few. In recognition of the sensitive nature of the information collected, federal law requires states to establish “safeguards which prohibit [its] use or disclosure,” with limited exceptions.¹³ Disclosure of SNAP data is permitted solely “for inspection and audit by the Secretary, subject to data and security protocols agreed to by the State agency and Secretary,” and for use in certain lawsuits by beneficiaries;¹⁴ “to persons directly connected with the administration or enforcement of” the federal SNAP statute “*only* for such administration or enforcement”;¹⁵ for use by the Comptroller General of the United States for audits;¹⁶ for law enforcement “for the purpose of investigating an alleged violation of” the SNAP statute or its regulations—but no other law enforcement purpose,¹⁷ except for certain fields that can be released to law enforcement to locate a fugitive;¹⁸ to garnish overpayments from the salaries of federal workers;¹⁹ for the state agency (not USDA) to report to the former

¹¹ 5 U.S.C. § 552a(a)(7).

¹² 7 C.F.R. § 273.2(f).

¹³ 7 U.S.C. § 2020(e)(8).

¹⁴ 7 U.S.C. § 2020(a)(3)(B).

¹⁵ 7 U.S.C. § 2020(e)(A) (emphasis added).

¹⁶ 7 U.S.C. § 2020(e)(B).

¹⁷ 7 U.S.C. § 2020(e)(C).

¹⁸ 7 U.S.C. § 2020(e)(E).

¹⁹ 7 U.S.C. § 2020(e)(8)(D).

Immigration and Naturalization Service (now Immigration and Customs Enforcement) that members of a household are ineligible to receive SNAP benefits because a person is in the United States unlawfully; or to address benefits paid to prisoners.²⁰

In setting out permissible purposes for state disclosure of SNAP data, Congress mapped the outer limits of what can be considered “compatible” with the original purposes of collection (i.e., program administration and eligibility determination). But several of the “routine uses” identified by USDA in the Notice would far exceed these limits, rendering them incompatible and invalid under the Privacy Act. For example, routine use (8) would confer effectively boundless authority on USDA to share SNAP data for law enforcement purposes: any record could be disclosed to any agency of any government merely because it “indicates” (in USDA’s unreviewable judgment) a “*potential* violation of [any] law, whether civil, criminal, or regulatory in nature.”²¹ This would impermissibly convert a federal benefit program into an all-purpose piggybank of personal data for use by law enforcement agencies, and it stands in marked contrast to the carefully circumscribed law enforcement disclosures permitted by Congress under 7 U.S.C. § 2020(e).

Routine use (11) is similarly unconstrained, purporting to allow USDA to disclose SNAP data to any domestic government that administers or investigates any benefits program supported by federal funds, so long as USDA believes the disclosure is “reasonably necessary . . . to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such programs.”²² This is a far cry from the relevant disclosures permitted by Congress under 7 U.S.C. § 2020(e), which are almost entirely tethered to *SNAP administration* and the prevention or investigation of *SNAP violations*.

²⁰ 7 U.S.C. §§ 2020(e)(8)(D), (e)(15), & (e)(18).

²¹ 90 Fed. Reg. 26,522 (emphasis added).

²² 90 Fed. Reg. 26,523.

Because multiple asserted “routine uses” in the Notice fail the Privacy Act’s compatibility requirement and pose serious privacy risks to SNAP recipients and applicants, the Notice is fatally defective and should be withdrawn.

III. The Notice reveals numerous other Privacy Act violations.

USDA’s problems go well beyond its assertion of invalid “routine uses.” Both the Notice and the NSID itself appear to violate multiple other provisions of the Privacy Act.

First, neither the Notice nor the established parameters of the NSID indicate that USDA has fulfilled its obligation to “collect information to the greatest extent practicable directly from” SNAP recipients and applicants,²³ even though SNAP data contained in the NSID may “result in adverse determinations about an individual’s rights, benefits, and privileges under [a] Federal program[.]”²⁴ By USDA’s own telling, the agency intends to use SNAP data “to identify and rectify any ineligible, duplicate, or fraudulent SNAP enrollments or transactions” and to “identify[] and eliminat[e] duplicate enrollments[.]”²⁵ Yet the Notice reflects no evaluation by USDA of whether it can carry out these same functions by collecting information directly from individuals (or by using existing program integrity tools like the National Accuracy Clearinghouse). Instead, USDA asserts without justification that it must undertake across-the-board consolidation of SNAP data from states and state vendors. This falls well short of the showing required by 5 U.S.C. § 552a(E)(2).

Second, although USDA cites generally to 7 U.S.C. § 2020 and two recent executive orders, the agency fails to establish that the creation of a new system of records (and the nationwide collection of SNAP data to populate that system) is “*necessary* to accomplish” any of USDA’s lawful obligations under those authorities.²⁶ Indeed, given that USDA can only legally obtain SNAP

²³ 5 U.S.C. § 552a(E)(2).

²⁴ 5 U.S.C. § 552a(E)(2).

²⁵ 90 Fed. Reg. 26,522.

²⁶ 5 U.S.C. § 552a(e)(1) (emphasis added).

data from states under “data and security protocols agreed to by the State agency and Secretary”²⁷—and given that USDA identifies no such protocols—it is unlikely that USDA could *ever* make the requisite showing of necessity for the sweeping collection of information described in the Notice. If anything, the proposed NSID threatens to significantly undermine the security of SNAP data that USDA is duty-bound to protect. Combining previously disaggregated datasets of personal information, particularly at the scale of a nationwide benefits program, exposes that data to heightened risk of breach by creating an attractive target and a single point of failure for fraudsters and other third parties to exploit. Nor can the SNAP data protections of Title 7 be superseded by an executive order, no matter how emphatically such an order insists on the consolidation of personal data. Whatever arguments USDA might raise to support the “necessity” of the NSID, USDA has certainly failed to make the showing required by 5 U.S.C. § 552a(E)(1) here.

Third, as noted in Part I, the Notice simply fails to identify a policy for the disposal of records contained in the proposed NSID, citing instead to a NARA records retention schedule that does not exist. This cannot satisfy USDA’s disclosure obligation under 5 U.S.C. § 552a(E)(4)(e).

Finally, the Notice states that information in the proposed NSID will be provided both by “the 53 State agencies that administer SNAP and their designated vendors” and by various unspecified “Federal agencies with which USDA partners on program integrity efforts[.]”²⁸ The consolidation of federal- and state-held personal data in a system used for “identifying and eliminating duplicate [SNAP] enrollments”²⁹ almost certainly constitutes a “matching program,” which includes any “computerized comparison of . . . a system of records with non-Federal records for the purpose of . . . establishing or verifying the eligibility of . . . beneficiaries of . . . cash or in-

²⁷ 7 U.S.C. § 2020(a)(3)(B)(i).

²⁸ 90 Fed. Reg. 26,522.

²⁹ 90 Fed. Reg. 26,522.

kind assistance or payments under [a] Federal benefit program[.]”³⁰ Yet the Notice does not identify any computer matching agreements between USDA and the relevant agencies that would authorize USDA to carry out the proposed consolidation. Absent such agreements, USDA’s establishment of a matching program using SNAP data would violate the computer matching restrictions of 5 U.S.C. § 552a(o).³¹

IV. Conclusion

For the above reasons, USDA should withdraw its Notice, abandon its proposal to establish the NSID, and halt its unlawful efforts to compel states and EBT vendors to turn over the confidential personal data of SNAP recipients and applicants. If you require any additional information about USDA’s Privacy Act and related statutory obligations, please contact John Davisson, EPIC Director of Litigation, at davisson@epic.org.

/s/ John Davisson
John Davisson
Director of Litigation

³⁰ 5 U.S.C. § 552a(a)(8).

³¹ 5 U.S.C. § 552a(o).