e: 3410-30-P

DEPARTMENT OF AGRICULTURE

Food and Nutrition Service

Privacy Act of 1974; Proposed New System of Records

AGENCY: Food and Nutrition Service (FNS), USDA.

ACTION: Notice of a proposed new privacy system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, and Office of Management and Budget (OMB) Circular No. A-108, notice is given that the Food and Nutrition Service (FNS) of the U.S. Department of Agriculture (USDA) is proposing to add a new system of records, entitled USDA/FNS-12, which will replace The Integrity Profile (TIP) as the system used to house State agency vendor management data for the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC). This system maintains records of activities conducted pursuant to FNS' mission and responsibilities authorized by legislation.

DATES: This notice is effective upon publication, subject to a 30-day notice and comment period in which to comment on the routine uses described below. Comments, if any, must be submitted by [insert date that is 30 days after publication in the Federal Register].

ADDRESSES: You may submit comments, identified by USDA/FNS-12, by one of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov provides the ability to type short comments directly into the comment field on this Web page or attach a file for lengthier comments. Follow the online instructions at that site for submitting comments.
- Mail: Amy Herring, Chief, Program Integrity & Monitoring Branch, Food and Nutrition Service, Braddock Metro Center II, 1320 Braddock Place, Office 3030, Alexandria, VA 22314.

- E-mail: SM.fn.FDPHelp@usda.gov
- Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.
- Docket: For access to the docket to read background documents or comments received go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact the FNS Privacy Officer via telephone at (703) 305-1627 or via e-mail at SM.fn.Privacy-FNS@usda.gov.

SUPPLEMENTARY INFORMATION:

Statutory Basis

The Statutory Basis for establishing the Food Delivery Portal (FDP) is Title 7. Agriculture of the Code of Federal Regulations, Section 246.12. Section 246.12 sets forth design and operational requirements for food delivery systems; makes State agencies responsible for the fiscal management of, and accountability for, the food delivery systems under its jurisdiction; provides FNS with oversight authority over State agencies; and dictates that all contracts or agreements entered into by the State or local agency for the management or operation of food delivery systems must conform to the requirements of 2 CFR part 200, subpart D, and USDA implementing regulations 2 CFR part 400 and part 415. Food delivery systems are defined as the method by which state and local agencies provide supplemental food to program participants.

Background

The FDP will replace the current TIP system, which was developed in fiscal year (FY) 2005 and has had no major upgrades since FY 2009. Although TIP exceeds industry standards for the software development life cycle, the current data structure and reporting interface make it difficult to conduct the meaningful data analysis necessary to provide effective federal oversight of WIC.

The data collected in TIP is critical to providing effective federal oversight of the WIC Program because the information informs FNS on State agency performance regarding vendor training, compliance, monitoring, and sanctions. TIP data may also be used by State agencies to assess trends in vendor compliance and identify areas for additional training and oversight.

FDP will include functionality that will improve program oversight and integrity in all areas of WIC vendor management, as well as address gaps found in the 2013 Office of Inspector General (OIG) audit. OIG found that two of the three State agencies that OIG visited were not properly monitoring and sanctioning vendors. FDP will collect monitoring and sanctioning information to enable FNS oversight of those activities. FDP will also reduce security risks, facilitate streamlined data collection methods, and utilize data analytics for early detection of fraudulent activities or State agency noncompliance.

Consistent with USDA's information sharing mission, information stored in FDP may be shared with other USDA components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after USDA determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this System of Records Notice.

FDP will replace TIP as the system used to house State agency data for the WIC Program. The information housed in FDP will be critical to providing effective federal oversight because the information informs FNS on State agency performance regarding vendor training, compliance, monitoring, and sanctions. FDP will improve program oversight and integrity in vendor management as well as addressing gaps found in the 2013 OIG audit report. FDP will also reduce security risks, facilitate streamlined data collection methods, and utilize data analytics for the early detection of fraudulent activities regarding State agency noncompliance.

Privacy Act

The Privacy Act of 1974 (the Privacy Act), 5 U.S.C. § 552a, embodies fair information

principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a system of records. A system of records is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the FDP system of records.

In accordance with 5 U.S.C. § 552a(r), USDA has provided a report of this new system to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: USDA/FNS-12, Food and Nutrition Service (FNS), Women, Infants, and Children (WIC) Food Delivery Portal (FDP).

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

The FDP is maintained in a cloud infrastructure environment that is used only by Federal employees and contractors and State agency employees and contractors. The data is processed and stored solely within the continental United States. Any paper records which contain PII are located in FNS Regional Offices throughout the United States. The location of each FNS Regional Office may be found in the local phone books or at https://www.fns.usda.gov/fns-

regional-offices.

SYSTEM MANAGER(S):

Amy Herring, Chief, Program Integrity & Monitoring Branch, Food & Nutrition Service, Braddock Metro Center II, 1320 Braddock Place, STE 3030, Alexandria, VA 22314, Amy.Herring@usda.gov, (703) 305-2376.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

7 C.F.R. § 246.12.

PURPOSE(S) OF THE SYSTEM:

The purpose of FDP is to house vendor management information submitted by State agencies. The information housed in the FDP will be critical to providing effective federal oversight, because the information informs the FNS on State agency performance regarding vendor training, compliance, monitoring, and sanctions. The FDP will replace The Integrity Profile (TIP), which is the legacy system used to house State agency vendor management data for WIC Program.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include USDA employees and contractors, store owners, and State agency users.

CATEGORIES OF RECORDS IN THE SYSTEM:

The following are the Categories of Records for FDP, which are all stored within various logical objects in FDP data model. The Contact object stores: the store's owner first and last name; system user first and last name; and an email address for each user. The FDE object stores: the store's tax identification number; the store's assigned Supplemental Nutrition Assistance Program (SNAP) number; and the store's assigned unique Salesforce ID. The Store Tracking and Redemption System (STARS) Store Data object stores: the store's tax

identification number and the store's assigned SNAP number.

RECORD SOURCE CATEGORIES:

Information in this system is provided to FNS by the State agencies that administer the WIC Program at the State level. If the State agency user provides a store's assigned SNAP number, then certain data is imported from the USDA STARS system. The data imported from STARS is the store's owner name(s); store's tax identification number; and the store's assigned SNAP number.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside USDA as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

(1) To the Department of Justice when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity where the Department of Justice has agreed to represent the employee; or (c) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records:

(2) To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

(3) When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising

by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate agency, whether Federal, foreign, State, local, or tribal, or other public authority responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutive responsibility of the receiving entity.

(4) Disclosure to contractors under section (m): To agency contractors, grantees, experts, consultants or volunteers who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 USC § 552a(m).

(5) Disclosure to NARA: Records from this system of records may be disclosed to the National Archives and Records Administration (NARA) or to the General Services Administration for records management inspections conducted under 44 USC § 2904 and § 2906.

(6) Information security breaches: To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(7) To WIC State agencies when a request is received, to provide back to them any information that originated from the State agency as a part of the normal usage of the

system. The FDP system will be used by WIC State agencies to provide data to the agency on WIC vendor management activities. The data provided will include store's business names; store's tax identification numbers; the store's assigned SNAP number; and the store's assigned unique Salesforce ID. The Supplemental Nutrition Assistance Program (SNAP) data disclosure to WIC State agencies: State agencies will be provided with data from the SNAP STARS system via FDP screens and reports. This data will only be provided if the WIC State agency provides an exact match of the agency number in SNAP's STARS system for a specific store. This information is provided to assist the State agency in determining program eligibility and ensuring program integrity in dually authorized stores.

(8) To another Federal agency or Federal entity, when USDA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The FDP will be hosted in a cloud infrastructure environment.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The user's permission level will dictate what records they can retrieve. Records can be retrieved by searching for the Food Delivery Entity (FDE) name, FNS Authorization Number, Federal Employer Identification Number (FEIN), or the State WIC ID (a.k.a. Vendor ID).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

FDP is a new System of Records that does not yet have a Records Schedule approved by the National Archives and Records Administration (NARA). The records within FDP will be retained indefinitely until NARA has approved a Records Schedule for FDP. The proposed Record Schedule for FDP dictates that records will be retained and disposed of in accordance

with the NARA General Record Schedules (GRSs) 3.1 and 5.2. GRS 3.1 applies to system documentation whereas GRS 5.2 applies to electronic and paper inputs and outputs. Records may be retained for a longer period as required by litigation, investigation, and/or audit. Electronic and/or paper records are retained with USDA employees and contractors at USDA offices.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

USDA safeguards records in this system according to applicable rules and policies, including all applicable USDA automated systems security and access policies. USDA has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

FDP utilizes a robust collection of technical safeguards to ensure the integrity of the platform. FDP is hosted in a secure server environment that uses a firewall to prevent interference or access from outside intruders. When accessing FDP, Secure Socket Layer (SSL) technology protects the user's information by using both server authentication and data encryption. FDP administrators will have a suite of security tools that can be used to increase the security of the system. From a physical security standpoint, the servers that host FDP are stored in a privately owned data center with strict physical access control procedures in place to prevent unauthorized access.

RECORD ACCESS PROCEDURES:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at http://www.da.usda.gov/foia_agency_pocs.htm. If an individual believes more than one

component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief FOIA Officer, Department of Agriculture, 1400 Independence Avenue, SW, Washington, D.C. 20250.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 7 CFR § 1.112. You must submit a written request in accordance with the instructions set forth in the system of records. The request should include the name of the individual making the request, the name of the system of records, any other information specified in the system notice, and when the request is one for access, a statement of whether the requester desires to make a personal inspection of the records or by supplied with copies by mail or email.

You must also include with your request sufficient data for FNS to verify your identity. If the sensitivity of the records warrant it, FNS may require that you submit a signed, notarized statement indicating that you are the individual to whom the records pertain and stipulating that you understands that knowingly or willfully seeking or obtaining access to records about another individual under false pretenses is a misdemeanor punishable by fine up to $5,000. No identification shall be required, however, if the records are required by 5 U.S.C. 552 to be released. If FNS determines to grant the requested access, fees may be charged in accordance with § 1.120 before making the necessary copies. In place of a notarization, your signature may be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their requests to the System Manager listed above. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same

record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES:

See RECORD ACCESS PROCEDURES.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

_____

Cynthia Long,
Administrator,
Food and Nutrition Service.
[FR Doc. 2021-21941 Filed: 10/6/2021 8:45 am; Publication Date: 10/7/2021]