Privacy Threshold Analysis
Guidance and Template

Policy and Directives

- Version: 1.0
- Date: May 19, 2020
- Prepared for: USDA FNS OIT

DOCUMENT ADMINISTRATION

Document Revision and History

Revision	Date	Author and Title	Office	Comments
3.1	August 2013	Staff	USDA OCIO-Policy and Directives - Privacy Office	Draft Version
Version 3.2	10 FEB 2014	Holly Beckstrom, IT Specialist	OCD/ASOC/USDA	Brought document into compliance with the USDA RMF terms and processes based on the SP800-37, Rev.1 specifications; for example replaced the term C&A with A&A.
3.2		LaWanda Burnette	OCIO-P&D – Privacy Office	Edits
3.5		L. Burnette	OCIO-PE&F	Add definition
3.6		L. Burnette	OCIO-PE&F	Factor Extend – A. Goldshine
4.0	October 2019	ITCON Services	OIT	Addition of project-specific information
5.0	June 2, 2020	OIT	OIT	Review of the FDP PTA with Miguel Marling (FNS Privacy Officer)

DOCUMENT REVIEW

Reviewer	Title	Date	Update: Y/N	If systemic, please provide comments
HJ Beckstrom	ASOC Section 508 Representative	02/10/2014	Y	Word and PDF versions of this document are certified Section 508 Compliant as of February 10, 2014.

Table of Contents

Introduction

The United States Department of Agriculture (USDA) is committed to preserve and enhance privacy protections for all individuals, to promote transparency of USDA operations, and to serve as a leader in the federal privacy community. The Privacy Threshold Analysis (PTA) is one step in fulfilling this commitment. The purpose of the PTA is to help program managers and system owners determine whether a Privacy Impact Assessment (PIA) is required under section 208 of the E-Government Act of 2002. A properly completed and reviewed PTA provides documentation that a system owner has assessed whether or not a full PIA is required. To appropriately protect the confidentiality of PII, organizations should use a risk-based approach, see the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information, (PII)*: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

In anticipation of NIST SP 800-53 revision 4, July 2012 or later, this PTA template is being revised to compliment and incorporate these changes. See NIST SP 800-53 rev 4: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Additional reference material can be found at USDA Privacy Council webpage:

The Privacy Council webpage (edited hypertext)

What is a PTA?

Privacy Threshold Assessments or PTAs are currently incorporated into the security assessment and authorization (A&A) process, formerly known as certification & accreditation (C&A) process. A&A is the process by which the Department assures its systems meet appropriate security and operating standards. Through the A&A process, the system owner completes the PTA and reviews it with the Agency Official for Privacy (AOP).

For all systems within USDA, a PTA must be conducted in order to determine if a full Privacy Impact Assessment (PIA) is necessary. The PTA and PIA are tools used to identify and qualify the extent of security measures needed to protect privacy and personally identifiable information (PII). Some information systems will not require a full PIA. Information owners or stewards can be aided in making the determination of whether a full PIA is required by work closely with the system owner or program manager to first conduct the PTA. For example, an agency may submit a PTA on a system that does not collect PII. The system will have an official PTA on file documenting the determination that a PIA is not required.

Agencies are required to review their privacy documentation, PTA, PIA, and System of Record Notice, (SORN), at a minimum, annually. Agencies are required to review

their PIA(s) and SORN(s) posted on the department's webpage on a reoccurring basis and immediately notify Privacy Office of any discrepancies.

The department's PIA(s) and SORN(s) are posted on the following webpages:

PIA:
http://www.usda.gov/wps/portal/usda/usdahome?contentid=Privacy_Impact_Assessment.xml&contentidonly=true

SORN: http://www.ocio.usda.gov/ocio_sor.html

The USDA Privacy Office can be contacted at privacy@usda.gov if there are any questions or concerns regarding this guidance

The Difference between a PTA and PIA

A PTA is not a PIA. A PTA simply helps determine whether or not a PIA needs to be completed. A PTA does not fulfill the requirements of the E-Government Act of 2002 which requires USDA to conduct a PIA before developing or procuring IT systems; or initiating projects that collect, maintain, or disseminate PII from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of PII.

Completing a PTA

The USDA has developed a PTA template to aid the Information Owner in determining whether or not a PIA needs to be completed, and for Departmental consistency and ease of use. The template includes questions to determine whether or not a PIA is required. These questions also consist of NIST 800-53 rev 4 privacy controls. The template is available as an appendix to this document and is also posted on the Privacy Council website. However, if a non-PDF version is needed, contact the USDA Privacy Office at privacy@usda.gov.

All PTAs completed after the effective date of this guidance must conform with the guidance contained herein and in the format provided in the template. All questions in the PTA template must be completed; please do not delete or modify sections of the template.

PTA Review Process

- As an initial step, the project manager or system owner should review the PTA with the Agency Official for Privacy (AOP) to ensure that the PTA was completed correctly and accurately.

- The agency then submits the completed PTA to the USDA Privacy Office via email at privacy@usda.gov. The USDA Privacy Office reviews the completed document regardless of whether it originated from a component or headquarters.
- If the USDA Privacy Office is in agreement with the submitted PTA, the next step would be to complete the PIA if needed. If there is any disagreement, the USDA Privacy Office will meet with the information owner/steward, project manager, system owner, and AOP, as necessary to review the PTA and make any appropriate changes. The agency can provide supplemental information to support their position which may consist of screen shots, data base field lists, etc.
- The approved PTA should be submitted during the initiation phase of the security assessment and authorization process.

Appendix A. Privacy Threshold Analysis Template

SUMMARY INFORMATION	
Date	June 22, 2020
Name of Project	Women, Infants, and Children Food Delivery Portal
Name of Component:	USDA FNS
Name of Information Owner/Steward:	Amy Herring
Phone of Information Owner/Steward:	703-305-2376
Email of Information Owner/Steward:	Amy.Herring@usda.gov
Name of Project Manager:	Marci Giordano
Phone for Project Manager:	703-605-0495
Email for Project Manager:	Marci.Giordano@usda.gov
Name of System Owner:	Amy Herring
Phone for System Owner:	703-305-2376
Email for System Owner:	Amy.Herring@usda.gov

1. Describe the project and its purpose:

Food Delivery Portal (FDP) will replace the current The Integrity Profile (TIP) system, which was developed in fiscal year (FY) 2005, and has had no major upgrades since FY 2009. Although the system exceeds industry standards for the software development life cycle (SDLC), the current data structure and reporting interface make it difficult to conduct meaningful data analysis necessary for Federal oversight of the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).

The data collected in TIP are critical to effective WIC oversight at the Federal level, because the information informs the Food and Nutrition Service (FNS) on WIC State Agency (SA) performance regarding vendor training, compliance, monitoring, and sanctions. TIP data may also be used by WIC SAs to assess trends in vendor compliance to 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 SAs 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 reduce security risks, facilitate streamlined data collection methods, and facilitate better use of data analytics for early detection of fraudulent activities, or SA noncompliance.

2. Status of Project:

☒ This is a new development effort.

☐ This is an existing project.

Date first developed: Scheduled Release Nov. 2020

Date last updated:

System in development currently is migrating the TIP application to Salesforce and building out a modernized system on the SNCS Salesforce Org.

3. Is the system in Cyber Security Assessment and Management (CSAM) C&A web?

☐ Unknown. (Please explain, in question 12)

☐ No.

☒ Yes.

Please list the system name and system identification number (must be the same as the system name/number in CSAM C&A web): WIC TIP was identification number 2391. Salesforce is 2497. A system identification number for FDP has not been designated.

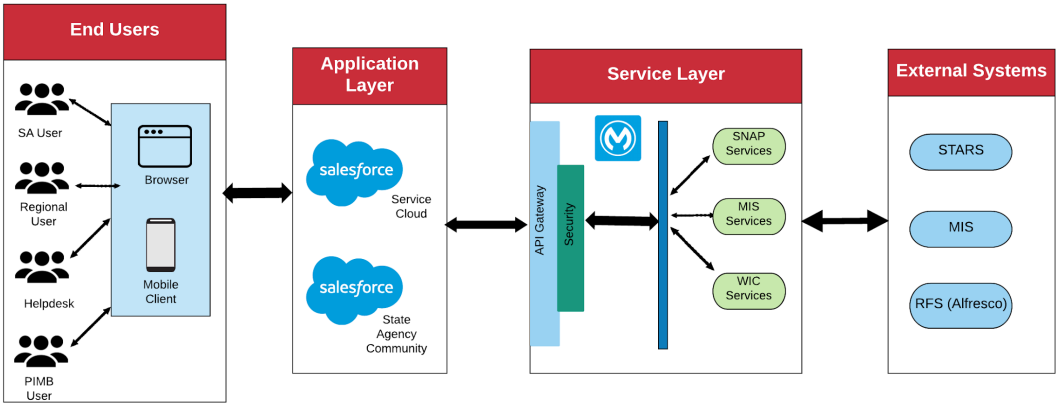
4. Is this system classified in CSAM as: (please select one)

☐ **Parent**

(_____)

☒ **Subordinate**

(Please attach a copy of the data flow diagram or database schema)



5. Is this a cloud system?

☐ No.

☒ Yes.

6. Is this a contractor system?

☐ No.

☒ Yes.

If yes, to questions 5 or 6, please select appropriate box:

☒ Contractor (internal)

☐ Contractor (external)

☐ Federal providing contracted services

If any of the boxes are checked, please provide name of vendor and URL if applicable: Vendor: ITCON Services; URL: On FNS Salesforce cloud; Domain Name ending in .usda.gov and Name is pending.

7. Does the system collect, process, generate or store PII information on: (Please check all that apply)

☒ USDA employees.

☐ Contractors or other entities working on behalf of USDA.

☐ Non-USDA Federal Government employees.

☒ USDA Partner.

☐ The general public.

☒ Other. (Benefactors, program participants, stakeholders, i.e. farmers, ranchers, producers, etc., these are still members of the public however, they have a degree of specific interest).

If others, please list: State Agency users

8. Does the system collect, process, generate or store any of the following information (that may be considered PII) on individuals: (Please check all that apply)

☒ Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias).

☐ Date and/or place of birth.

☒ Address Information (street or email address).

☒ Personal identification number (e.g. social security number, tax identification number, passport number, driver's license number or a unique identification number, etc)

☐ Financial data (credit card numbers, bank account numbers, etc.).

☐ Health data (including height, weight, blood pressure, etc.).

☐ Biometric data (fingerprints, iris scans, voice signature, facial geometry, DNA, etc.).

☐ Criminal history.

☐ Employment history.

☒ Miscellaneous identification numbers (agency assigned number, case number, accounts, permits, etc.).

☐ Photographic image/identifying characteristics.

☐ Handwriting or an image of the signature.

☒ Other information that may be seen as personal (personal characteristics, etc.).

If so, please list: It is a store number identifier

9. Does the system use or collect Social Security Numbers (SSNs) or Tax Identification Numbers, (TINs)? (This includes truncated SSNs/TINs e.g. last 4 digits)?

☒ No.

☐ Yes.

If yes, why does the project collect SSNs or TINs? Provide the function of the SSN/TIN and the legal authority to do so:

9a. **Does the system utilize the following security controls?**

☒ Encryption.

☐ Masking of PII data.

☒ Controlled access.

☒ Timeout for remote access.

☒ System audit logs.

10. Does the system require the user to enter a user name and password in order to gain access to the system (e.g. e-Authentication)?

☐ No. (Please explain.)

☒ Yes.

If yes, please describe the authentication process: e-Auth and a 674 process

11. Does the system connect, receive, or share PII[1] with any other USDA systems?

☒ No.

☐ Yes.

If yes, please list the other USDA systems:

12. Does the system connect, receive, or share PII with any non-USDA systems?

[1] Personally Identifiable Information (PII) is information that can identify a person. This may include: name, address, phone number, social security number, image, as well as health information or a physical description.

☒ No.

☐ Yes.

If yes, please list the non-USDA systems:

13. **Matching records via computer/automated process, performed by federal agency, whether the personal records used in the match are federal or non-federal PII. Reference DR 3450-001:** http://www.ocio.usda.gov/directives/doc/DR3450-001.pdf

a. Are you comparing two or more PII records or system of records?

☒ No.

☐ Yes

b. Are you comparing any system of record with non -federal records?

☒ No.

☐ Yes

If yes, for question 13a or 13b, the efforts or purpose have to meet at least one of these conditions:

- Creating or checking eligibility or compliance with laws/regulations of applicants or recipients/beneficiaries of a federal program/grant.

  OR

- Recouping payments, delinquent debts or overpayments owed to government agencies from a federal benefit program.
  OR

- Two or more automated Federal personnel or payroll systems of records or a system of Federal Personnel of payroll records with non-federal records.

Exclusions for the conditions above: *Aggregate statistical, research or statistical project, enforcement of criminal laws, tax information, etc. Please see PL 100-503, Computer Matching Act for specific details.*

c. Based on the responses above, is a CMA required?

(Affirmative for 13a. or 13b and either of the options for efforts are met),

☐ No. (Skip to question 15)

☐ Yes. (Please respond to question 14, if "yes").

14. **Do you have a Computer Matching Agreement?**

☒ No.

☐ Yes. (Please list this agreement on the Privacy Council webpage posting)

15. Are there regular (e.g. periodic, recurring, etc.) PII data extractions from the system?

☒ No.

☐ Yes.

(Reference Memorandum – posted on website)

If yes, have proper controls and policies been developed to address the data logging requirements outlined in Office of Management and Budget (OMB) Memorandum
M-07-16, "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*"?

☐ No.

☐ Yes.

16. Does the system track or measure the browsing habits or preferences of the public or user? (refer to OMB Memoranda M-10-22 "*Guidance for Online Use of Web Measurement and Customization Technologies*" and M-10-23 "*Guidance for Agency Use of Third-Party Websites and Applications*")

☒ No.

☐ Yes.

If yes, have proper controls and policies been developed to meet all the requirements outlined in Office of Management and Budget (OMB) Memoranda M-10-22 "*Guidance for Online Use of Web Measurement and Customization Technologies*" and M-10-23 "*Guidance for Agency Use of Third-Party Websites and Applications.*"

☐ No.

☐ Yes

17. Is application/system mobile device compatible? (Y/N)

☒ No.

☐ Yes

If none of the boxes were checked for questions number 7 – 8 and **"NO"** was answered for questions 9, 11, and 12, **DO NOT** complete a PIA for this system.

If any box was checked for questions number 7 - 8, and any answers to questions 9 through 12 were "**YES**," A PIA **MUST** be completed for this system.

PIA REQUIRED	
YES	NO
X	

(Check one)

Privacy Office reserves the right to request additional information during the review of privacy documentation for the systems.

Signature authority and protocol differs by agency, we request at a minimum Project Manager/System Owner and ISSPM/CISO sign the document with review by the Privacy Officer.

Agency Responsible Officials

MARCI GIORDANO Digitally signed by MARCI GIORDANO
Date: 2020.08.27 09:09:35 -04'00'

Marci Giordano
Project Manager
Program Integrity and Monitoring Branch
Food and Nutrition Service
United States Department of Agriculture

Date

KELLY JACKSON Digitally signed by KELLY JACKSON
Date: 2020.08.28 09:55:34 -04'00'

Kelly Jackson
Information Owner
Program Analyst, Program Integrity and Monitoring Branch Food and Nutrition Service
United States Department of Agriculture

Date

Agency Approval Signature

JOSEPH BINNS Digitally signed by JOSEPH BINNS
Date: 2020.08.28 13:02:19 -04'00'

Joseph Binns
ISSPM\CISO
Food and Nutrition Service
United States Department of Agriculture

Date

Appendix B. Acronyms

Acronyms used in this document are listed below in alphabetical order.

Acronym	Description
A&A	Assessment and Authorization (formerly Certification & Accreditation)
AOP	Agency Official for Privacy
CMA	Computer Matching Agreement
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management
EOM	End of Month
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PTA	Privacy Threshold Analysis
SAOP	Senior Agency Official for Privacy
SORN	System of Record Notice
SP	Special Publication
SSN	Social Security Number
SSP	System Security Plan
TIN	Tax Identification Number
USDA	United States Department of Agriculture (often referred as “Department”)

Appendix C. DEFINITIONS:

Term	Definition
Computer Matching Agreement, CMA	The Computer Matching and Privacy Protection Act covers two kinds of matching programs: (1) matches involving Federal benefits programs; and, (2) matches using automated records from Federal personnel or payroll systems of records.
Generate	Generate is defined as the creation of an item. For the purpose of privacy documentation, generate in terms of the system creating PII data.
Process	Process is defined as a method or action that results in a transformation or alteration of data. For the purpose of privacy documentation, system manipulate or change the PII data within the system.
Third party websites/applications	The term "third-party websites or applications" refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website.
Store	Store is defined as a location in which data is retained. For the purpose of privacy documentation, system contain or maintain for future access PII data.

Appendix D. NIST SP 800-53 Revision 4 Appendix J

Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. There are eight privacy control families with each family aligning with one of the Federal Information Processing Standards (FIPS.) The privacy control families can be implemented at the organization, department, agency, component, office, program, or information system level, under the leadership of the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO)[2] and in coordination with the Chief Information Security Officer (CISO), Chief Information Officer (CIO), program officials, and legal counsel. Table J-1 provides a summary of the privacy controls by family in the privacy control catalog

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

CNTL NO.	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information

[2] All federal agencies and departments designate an *SAOP/CPO* as the senior organizational official with the overall organization-wide responsibility for information privacy issues. OMB Memorandum 05-08, provides guidance for the designation of SAOPs/CPOs.

CNTL NO.	PRIVACY CONTROLS
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Source:
NIST Special Publication 800-53-Rev.4, *Security and Privacy Controls for Federal Information Systems and Organizations*