Privacy Threshold Analysis

Guidance and Template



* Version: 1.3
* Date: August 15, 2013
* Prepared for: USDA OCIO-Policy and Directives - Privacy Office

Policy and Directives

**DOCUMENT ADMINISTRATION**

Document Revision and History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Revision | Date | Author and Title | Office | Comments |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

DOCUMENT REVIEW

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reviewer | Title | Date | Update: Y/N | If systemic, please provide comments |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Introduction 1](#_Toc330911840)

[What is a PTA? 1](#_Toc330911844)

[The Difference between a PTA and PIA 2](#_Toc330911845)

[Completing a PTA 2](#_Toc330911846)

[PTA Review Process 2](#_Toc330911847)

[Appendix A. Privacy Threshold Analysis Template 3](#_Toc330911848)

[Appendix B. Acronyms 9](#_Toc330911851)

[Appendix C. DEFINITIONS: 10](#_Toc330911852)

[Appendix D. NIST SP 800-53 Revision 4 Appendix J 11](#_Toc330911853)

# 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 NIST 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://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>

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

# [The Privacy Council webpage (edited hypertext)](http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/ppii/ppii.privacy_council/!ut/p/c5/hc5JDoJAEAXQs3CCqk430L1EkVkGERA2BBMlhMmF4fw2cWNI1Krly69fUIHcqVm6tnl289QMcIFKq3dnM1YDnRHbCBHdJBCObyGirkkvtTrmxzwPzpRwKyTo-iwhJokpcvyTLqDcgwdVO8xXWVas9R8BjDJ5LhGEM)

# What is a PTA?

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

Some information systems will not require a full PIA. For efficiency, a system owner or program manager can be aided in making the determination of whether a full PIA is required by conducting and following a PTA. For all systems within USDA, a PTA must be conducted in order to determine if a full PIA is necessary.

For example, an agency may submit a PTA on a system that does not collect Personally Identifiable Information (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. The 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) can be found here:

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](file:///C:/Documents%20and%20Settings/lburnette/My%20Documents/StLDrive/My%20Documents/OCIO%20-%20TP&E%20(Mrs.%20Yvonne%20Jackson)/PTA_PIA_Checklists/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 program manager or system 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. 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 AOP to ensure that the PTA was completed correctly and accurately.
* The agency then submits the completed PTA to the USDA Privacy Office at [privacy@usda.gov](mailto: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 project manager or system owner and AOP, the next step would be to complete the PIA. If there is any disagreement, the project manager or system owner, AOP, and the USDA Privacy Office will meet 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 C&A process.

1. Privacy Threshold Analysis Template

|  |  |
| --- | --- |
| **Summary Information** | |
| **Date** | *<Please enter date submitted for review>* |
| **Name of Project** | *<Please enter the project name.>* |
| **Name of Component:** | *<Please enter Component Agency or Staff Office name.>* |
| **Name of Project Manager:** | *<Please enter the name of Project Manager.>.* |
| **Phone for Project Manager:** | *<Please enter the phone number for Project Manager.>* |
| **Email for Project Manager:** | *<Please enter the email address for Project Manager.>* |
| **Name of System Owner:** | *<Please enter System Owner’s name.>* |
| **Phone for System Owner:** | *<Please enter System Owner’s telephone number.>* |
| **Email for System Owner:** | *<Please enter System Owner’s email address.>* |

1. **Describe the project and its purpose:**

*<Add a general description of the project and its purpose in a way a non-technical person can understand.>*

1. **Status of Project:**

This is a new development effort.

This is an existing project.

Date first developed:

Date last updated:

*<Add a general description of the update.>*

1. **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): *<Add list here>*

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

**Parent**

**(***Please list here:* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)**

**Child**

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

1. **Is this a cloud system?**

No.

Yes.

1. **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:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **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: *<Add list here>*

1. **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: *<Add list here>*

1. **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: *<Add reason and legal statue granting the agency/organization the authority to collect this information here>*

*Please validate this system is part of the SSN/TIN Initiative for OMB M 07-16 on Privacy Council webpage.*

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

Encryption.

Masking of PII data.

Controlled access.

Timeout for remote access.

System audit logs.

1. **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 <*Add here>*

1. **Does the system connect, receive, or share PII[[1]](#footnote-1) with any other USDA systems?**

No.

Yes.

If yes, please list the other USDA systems: *<Add list here>*

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

No.

Yes.

If yes, please list the non-USDA systems: *<ADD list here>*

1. **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>
   1. **Are you comparing two or more PII records or system of records?**

No.

Yes

* 1. **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 14)

Yes. (Please respond to question 13, if “yes”).

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

No.

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

1. **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.

1. **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

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

No.

Yes

If none of the boxes were checked for questions number 7 – 8 and **“NO”** wasanswered 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 11 were “**YES**,” A PIA **must** be completed for this system.

|  |  |
| --- | --- |
| **PIA Required** | |
| **Yes** | **No** |
|  |  |

(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

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*< ADD Project Manager/System Owner>, <Date>*

*<ADD Component/Office>*

United States Department of Agriculture

# Agency Approval Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name Date

Title

United States Department of Agriculture

1. Acronyms

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

| **Acronym** | **Description** |
| --- | --- |
| AOP | Agency Official for Privacy |
| C&A | Certification and Accreditation |
| 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 |
| SORN | System of Record Notice |
| SSN | Social Security Number |
| SSP | System Security Plan |
| TIN | Tax Identification Number |
| USDA | United States Department of Agriculture (often referred as “Department”) |

1. DEFINITIONS:

|  |  |
| --- | --- |
| 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. |
| 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. |

1. NIST SP 800-53 Revision 4 Appendix J

(Projected scheduled release date of EOM August 2012):

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 FIPPs. 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]](#footnote-2) and in coordination with the Chief Information Security Officer, Chief Information Officer, 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 |
| 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-Rev4 Security and Privacy Controls for Federal Information

Systems and Organizations

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. [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)