PRIVACY RISK MANAGEMENT

COLLECTIONS, PIAS, AND SORNS

CHAPTER 01

HANDBOOK	ITS-HBK-1382.03-01
EFFECTIVE DATE:	20120925
EXPIRATION DATE:	20180820
RESPONSIBLE OFFICE:	OCIO/ IT SECURITY DIVISION

Distribution:

NODIS

Approved

Robert Binkley
Associate CIO for IT Security (Acting)

10-6-2015
Date

Change History

Version	Date	Change Description
1.0	9/25/2012	Initial draft
1.1	8/31/2015	Reviewed and approved by the acting associate CIO for IT Security

Table of Contents

Index

Overview

This handbook outlines the National Aeronautics and Space Administration (NASA) processes and procedures for collecting Personally Identifiable Information (PII), conducting Privacy Impact Assessments (PIAs), developing System of Records Notices (SORNs) and Privacy Act (e)(3) Statements (Privacy Act Statements). In addition, the handbook outlines the required privacy actions by information stage.

> PII is defined in Office of Management and Budget (OMB) Memorandum M-07-16 as "…information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." In accordance with OMB Memorandum M-10-23, "… [t]he definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information , could be used to identify an individual."

Every NASA user has the responsibility to protect PII that is entrusted to NASA. Additionally, Information Owners (IOs) and Information System Owners (ISOs) have an obligation to ensure that privacy requirements for collections of PII, PIAs, SORNs, Privacy Act Statements, and Computer Matching Agreements are met. Specifically, IOs and ISOs are responsible for:

- IOs collecting PII: Utilizing the Privacy & Controlled Unclassified Information (CUI) Assessment Tool (PCAT) to determine what privacy requirements are applicable.
- ISOs (regardless of whether or not PII is collected): Conducting an Initial Privacy Threshold Analysis (IPTA) in PCAT for each application, website, information system or collection of information within their purview to determine what, if any, privacy requirements are applicable. If PCAT indicates a PIA is required, the ISO is responsible for processing a PIA.
    - According to NASA Procedural Requirement (NPR) 1382 *NASA Privacy Procedural Requirements,* "NASA conducts PIAs under two circumstances: (1) in accordance with Section 208 of the e-Government (e-Gov) Act of 2002 and [National Institute of Standards and Technology (NIST) Special Publication (SP)] 800-53, for any new or substantially changed information system[s] that collect, maintain, or disseminate Information in Identifiable Form (IIF)] from or about members of the public, (under the e-Gov Act, members of the public exclude Government personnel, contractors, and partners); or, (2) in accordance with the Paperwork Reduction Act (PRA) for a new collection of 10 or more members of the public." Additionally, a PIA is required for any NASA use of Third-Party applications and websites (e.g., Facebook, Twitter).

1. Introduction

This handbook is designated by *NPR 1382.1* as providing implementation guidance for the privacy risk management and compliance requirements. The handbook is designed to act as a guide to IOs and ISOs as they navigate the PII collection process – including information on conducting a PIA and developing a SORN and a Privacy Act (e) (3) Statement.

Applicable Documents

- *e-Gov Act of 2002, as amended, 44 United States Code (U.S.C.) §§ 101 et seq.*
- *Children's Online Privacy Protection Act of 1998 (COPPA), 15. U.S.C. §§6501 et seq., 16 Code of Federal Regulations (C.F.R) § 312.*
- *PRA, 44 U.S.C. § 3501, et seq.*
- *OMB Circular No. A-130, Federal Agency Responsibilities for Maintaining – Appendix I Records About Individuals*
- *OMB Memorandum M-03-22,* OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- *OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- *OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications*
- *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.*
- *Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*
- *NASA Policy Directive (NPD) 1382.17, NASA Privacy Policy*
- *NPR 1382.1, NASA Privacy Procedural Requirements*
- *ITS-HBK-1382.03-02, Privacy Risk Management and Compliance: Annual Reporting Procedures for Reviewing and Reducing PII and Eliminating the Unnecessary Use of [Social Security Numbers (SSN)].*
- *Information Technology Security Handbook (ITS-HBK)-1382.06-01, Privacy Notice and Redress*
- *NASA Form (NF) 1534, Privacy Act Cover Sheet*
- *NF 1686, Sensitive But Unclassified*
- *NF 1536, Privacy Act Disclosure Authorization And Accounting Record (DAAR)*

2. PII Defined

2.1. PII is defined in Office of Management and Budget (OMB) Memorandum M-07-16 as "…information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." In accordance with OMB Memorandum M-10-23, "… [t]he definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that

non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information , could be used to identify an individual."

2.2. NASA makes a distinction between Sensitive and Non-Sensitive PII. Sensitive PII should be protected in accordance with the NASA sensitive information (e.g., Sensitive But Unclassified (SBU)/CUI) requirements.

2.2.1. ***Non-Sensitive PII***: Non-Sensitive PII is information that is available in public sources and the disclosure of which cannot reasonably be expected to result in personal harm.

> Examples of Non-Sensitive PII include name, work e-mail, work phone, work address. However, these elements when combined with sensitive PII may then become sensitive PII.

2.2.2. ***Sensitive PII***: Per NPR 1382.1A, sensitive PII is a combination of PII elements, which if lost, compromised, or disclosed without authorization, could be used to inflict substantial harm, embarrassment, inconvenience, or unfairness to an individual.

> Sensitive PII is any information or compilation of information [aggregate collection], in electronic, non-electronic, or … [other] form that includes:
> (1) an individual's first and last name or first initial and last name in combination with any of the following data elements:
> a) Home address or telephone number; [(including personal cell phone numbers and personal e-mail addresses)]
> b) Mother's maiden name;
> c) Month, day, and year of birth;
> (2) A social security number (in whole or in part), driver's license number, passport number, or alien registration number or other government-issued unique identification number;
> *Note:* A Universal Uniform Personal Identification Code (UUPIC) is not considered sensitive PII.
> (3) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation;
> (4) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code;
> (5) Any combination of the following data elements:
> a) An individual's first and last name or first initial and last name;
> b) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or
> c) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

3. Information in Identifiable Form (IIF) Defined

As outlined in *NPR 1382*, section 208(d) of the e-Gov Act of 2002 defines Information in Identifiable Form (IIF) as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." In accordance with OMB Memorandum M-03-22, IIF "is information in an IT system or online collection: (i) that directly identifies an individual (e.g. name, address, social security number or other identifying number or code, telephone number, e-mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)." IIF collected on members of the public requires a full PIA.

4. Privacy Actions by Information Stage

This section may be utilized by information owners to track their privacy responsibilities through the system development lifecycle. The bulleted items in the following sections identify the actions required during each stage.

4.1. Application/ Website/ Information System Planning/Development (Lifecycle)

4.1.1. The deciding factors for determining the privacy requirements for applications, websites, or information systems must be understood during the earliest stage of the lifecycle process (planning and development). These factors are: 1) the type of information to be collected and maintained; and, 2) how the information is managed. The privacy requirements must be met prior to release of the application, website or information system into production for use.

- ❑ Data Categorization – FIPS 199 security categorization[1]
- ❑ Conduct an Initial Privacy Threshold Analysis (IPTA).[2]
  - ❑ PIA indicated → Conduct a PIA. *See Section 6 for information on the PIA process*.
- ❑ Determine if the system will contain a Privacy Act System of Record (SOR).[3]
  - ❑ Yes → Publish a SORN in the Federal Register. *See Section 7 for information on the SORN process*.
- ❑ Determine if an OMB PRA authorization is required.[4]
  - ❑ Yes→ Work with the NASA PRA Clearance Officer to obtain an OMB Control number.

[1] In accordance with NPR 1382 §4.2.4.c., ensure any sensitive PII is categorized at a minimum level of Moderate for Confidentiality.

[2] The online privacy system (PCAT) should be used for the IPTA. PCAT was developed by the Office of the Chief Information Officer (OCIO) Information Technology Security Division (ITSD) to streamline the privacy planning/development process.

[3] This will be accomplished through the completion of an IPTA within the online privacy system (PCAT).

[4] *Id*.

- ❑ Determine if Web Measurement and Customization Technology (Persistent Tracking) will be used and whether or not an approval or waiver will be required.[5]

4.2. Collecting Personally Identifiable Information Requirements

4.2.1. As outlined in *NPR 1382.1*, NASA may only collect/ maintain the minimum necessary information about individuals which is relevant and necessary to accomplish a NASA purpose.

- ❑ Determine what notification requirements are required for the application/ website/ information system.
  - ❑ Collecting from Members of the Public → e-Gov Act applies. *See ITS-HBK-1382.06-01 Privacy Notice and Redress*.
  - ❑ Collecting from minors under the age of 13 → COPPA applies. *See ITS-HBK-1382.06-01 Privacy Notice and Redress*.
  - ❑ Retrieval is by Name or Unique Identifier → Privacy Act applies. *See ITS-HBK-1382.03-01, Section 7*.

4.3. Maintenance Requirements

- ❑ Ensure information is maintained, current, accurate, relevant, and complete.
- ❑ Protect against unauthorized alteration, access, use, or disclosure.
- ❑ Ensure system security controls related to privacy are implemented as identified in *NPR 1382.1, 2810.1,* and the related handbooks.

4.4. Utilization Requirements

- ❑ Limit use to those described in the SORN, PIA, and website policy statements, etc.
- ❑ Limit access to employees that have a need to know the information for the performance of their duties.
- ❑ Disclose Privacy Act records only pursuant to the routine uses published within the SORN.
- ❑ Notify users at entry to electronic SOR that the application/website/information system contains PII that must be protected and not disseminated without authorization.
- ❑ Train employees on their responsibilities regarding access, use, dissemination, protection and reporting of breaches of PII.

4.5. Dissemination Requirements

- ❑ Limit PII dissemination, sharing, and disclosure of the information to:
  - Purpose for which the information was collected.
  - Routine use described in the SORN.
  - NASA employees who require the information to accomplish their jobs.
  - Compliance with written consent requirements.
- ❑ Encrypt all sensitive PII in accordance with NASA sensitive information (e.g., SBU/CUI) policy.

[5] *Id*.

- ❑ Utilize *NF 1534*, *Privacy Act Cover Sheet*, when transmitting hard copy privacy data that is subject to the Privacy Act.
- ❑ Utilize *NF 1686*, *Sensitive But Unclassified* Cover Sheet, when transmitting all hard copy sensitive privacy data.
- ❑ Utilize *NF 1536*, *Privacy Act DAAR*, when disclosing Privacy Act SOR data.

4.6. Disposition Requirements

- ❑ Dispose of Federal records in accordance with the NASA Records Retention Schedule (NRRS) or General Records Schedule (GRS).

5. Collecting PII

NASA is permitted to collect PII under limited circumstances. IOs and ISOs are encouraged to work with their Center Privacy Manager (CPM) during the development phase to determine whether or not the collection is permissible.

- Requirements for collecting PII: **The collection must be (1) legally authorized (there is a law, regulation, or Government-wide policy that permits the collection), (2) necessary for the proper performance of a NASA function/mission, and (3) to the minimum extent necessary.**
  - Collections of PII are not authorized unless there is a clear, documented need for the information and an established authority for doing so. This also means that the collection of any privacy information beyond that which is absolutely necessary for the project/program to function is prohibited. All elements of PII collected should be used; any unused data element should not be collected.

On an annual basis, IOs and ISOs are required to review and determine whether the collection can be reduced[6] or eliminated.

5.1. Collecting PII Roles and Responsibilities

5.1.1.*The CPM shall*: [7]

- Ensure all collections of PII at their Center meet the requirements in *NPR 1382.1* and this handbook.

5.1.2.*The ISO shall*:

- Meet the requirements outlined in *NPR 1382.1* for Collecting PII.
- Utilize the PCAT application to determine what privacy requirements are applicable to the collection of PII and make the appropriate registrations.
- Conduct "review and reduce" activities as outlined in *ITS-HBK-1382.03-02*.

[6] Information on the IOs/ISOs annual Review and Reduce responsibilities and process associated with each collection can be found in IT*S-HBK-1382.03-02, Privacy Risk Management and Compliance: Annual Reporting Procedures for Reviewing and Reducing PII and Eliminating the Unnecessary Use of SSN*.

[7] The terms "shall" and "may" within this handbook are used as defined in ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks.

5.1.3.*The IO shall:*

- Meet the requirements outlined in *NPR 1382.1* for Collecting PII.
- Utilize the PCAT to determine what privacy requirements are applicable to the non-electronic record collecting PII (including all forms).
- Conduct review and reduce activities as outlined in *ITS-HBK-1382.03-01*.

6. PIAs

The e-Gov Act requires federal agencies to conduct an analysis of how information within the agency is handled to ensure compliance with applicable legal, regulatory, and policy requirements that apply to privacy related information, when collected by or on behalf of the government. To determine the risks, effects and related compliance requirements associated with collecting, maintaining, and disseminating privacy information in electronic information systems, and to examine and evaluate protections and processes for handling information and mitigate potential privacy risks, NASA requires IPTAs on all applications, websites, and information systems at NASA. An IPTA is required for all new collections, applications, websites, and/or systems, as well as all pre-existing collections, applications, websites, and/or systems that have not been previously assessed. This process serves to identify and initiate the completion of a full PIA when required. A completed IPTA/PIA demonstrates that NASA considers privacy from the beginning stages of a collection or system's development and throughout the collection's life cycle (i.e., collection, use, retention, processing, disclosure, and destruction). This analysis ensures that privacy protections are built into the collection from the start, not after the fact, when they can be far more costly or could affect the viability of the project. Additionally, the IPTA and PIA process demonstrates that the system developers and collection owners have made choices that reflect the incorporation of privacy into their collections. Further, a completed PIA gives the public notice of this analysis and helps promote trust between the public and NASA.

PCAT shall be used for conducting the IPTA and PIAs required by *NPR 1382.1*. PCAT is available at: https://pcat.nasa.gov.

6.1. IPTA/PIA Roles and Responsibilities

6.1.1.*The Senior Agency Official for Privacy (SAOP) shall*:

- Meet the requirements outlined in *NPR 1382.1* for PIAs.
- Develop the IPTA and PIA questions in accordance with requirements of Section 208 of the e-Gov Act section "II. Privacy Impact Assessment."

6.1.2.*The NASA Privacy Programs Manager shall*:

- Conduct activities to ensure NASA is in compliance with *NPR 1382.1* for collecting PII.
- Review PIAs for accuracy and completeness in a timely fashion.
- Ensure that the OCIO PIA review is conducted in a timely fashion.
- Ensure that all completed PIAs are published for the public on the NASA website http://www.nasa.gov/privacy/PIA.html.

6.1.3. *The NASA Privacy Act Officer shall*:

- Meet the requirements outlined in *NPR 1382.1* for collecting PII.
- Review the relevant compliance sections of IPTAs and PIAs that are subject to the Privacy Act.

6.1.4. *The CPM shall*:

- Meet the requirements outlined in *NPR 1382.1* for collecting PII.
- Review all IPTAs and PIAs in a timely fashion.
- Work with ISOs and IOs to ensure the IPTA and PIA is accurate and complete.

6.1.5. *The ISO shall*:

- Meet the requirements outlined in *NPR 1382.1* for collecting PII.
- Conduct an IPTA in PCAT for each application, website, information system or information collection,[8] or when a system undergoes a major change.
- Conduct a PIA in PCAT for each application, website, or information system, as appropriate.[9]
- Conduct a PIA in PCAT for each instance of third-party application/website use.
- Ensure that PIAs are updated in PCAT to reflect changes in authority, ownership, process, procedure or content.

6.1.6. *The IO shall*:

- Meet the requirements outlined in *NPR 1382.1* for collecting PII.
- Conduct an IPTA in PCAT for each non-electronic collection of PII.

6.1.7. *The PRA Clearance Officer shall*:

- Meet the requirements outlined in *NPR 1382.1* for collecting PII.
- Review PIAs that relate to the PRA and provide concurrence within PCAT.

6.1.8. *The Center Records Manager may* review records retention schedules identified within PCAT.

6.2. IPTAs

6.2.1. What is an IPTA?

Completion of an IPTA assists the collection owner in determining whether their information collection requires a PIA and initiates the collection of PII into the NASA PII collections inventory. In many cases, simply completing an IPTA will satisfy the privacy analysis as required by NPR 1382.1.[10] In other cases, a completed PIA will be needed to conduct a more in depth analysis of their collection. The responsibility to conduct an IPTA lies with the collection owners (IOs and ISOs) for all collections, electronic or non-

[8] See Section 5 of this handbook for information on collections of PII.
[9] PCAT analysis will result in the determination of when a PIA is required.
[10] In addition, the IPTA determines whether a collection is within the scope of the Privacy Act, the e-Gov Act, or the Paperwork Reduction Act and other NASA, Federal, or government-wide policies.

electronic. Conversely, the responsibility for a PIA is specific to the collection owner (ISO) if the collection is part of an electronic information collection.

6.2.2. When to Conduct an IPTA

IPTAs should be conducted at the beginning of the system, application, or information collection development lifecycle, prior to procurement, or modification. An IPTA shall also be conducted for all legacy collections, applications, websites or systems that are operational but do not have an IPTA documented. The IPTA will determine whether a PIA is required and will inform ISOs and IOs of what compliance endeavors are required.

6.2.3. When to Update an IPTA

An IPTA shall be updated when there has been a substantial change made to the application, website, or information system.

- General Rule of Thumb for Updating an IPTA: **Any noteworthy change to the information being collected or any portion of the information handling and management process for an application, website, information system, or collection requires a review and update of the IPTA**.

An update is required when there are new uses of existing information collections, including: application of new technologies, significant changes in how PII is managed, change in whom PII is being collected from, changes in the duration of information retention, or changes in how the information is being collected (e.g., forms, electronic, non-electronic). The update to the IPTA may result in a full PIA being required.

6.3. PIAs

6.3.1. What is a PIA

A PIA analyzes how PII is collected, used, stored, and protected by NASA and serves as documentation that the collection is being conducted in full compliance with applicable federal laws, statutes, government-wide and NASA policies and procedures. In addition, the PIA examines the risk to the individual caused by the collection of IIF. The PIA answers the following questions:

- What IIF is being collected by NASA?
- What is the legal authority for collecting the IIF?
- Is the collection within the bounds of that authority?
- Is the information the minimum needed for the authorized purpose?
- How will the IIF will be used and shared?
- Is the information appropriately secured and managed?
- How can the information be accessed?

The PIA is published to the public-facing NASA website to demonstrate to the public how NASA has incorporated all necessary privacy protections.

6.3.2. When to Conduct a PIA

In accordance with the requirements of *NPR 1382.1*, a PIA shall be conducted for:

- Any new, previously un-assessed, or substantially changed application, website, or information system that collects, maintains, or disseminates IIF from or about members of the public (under the e-Gov Act, "members of the public" exclude government personnel, contractors, and partners).
- A collection of IIF that is subject to the PRA.
- NASA use of a third-party application or website.

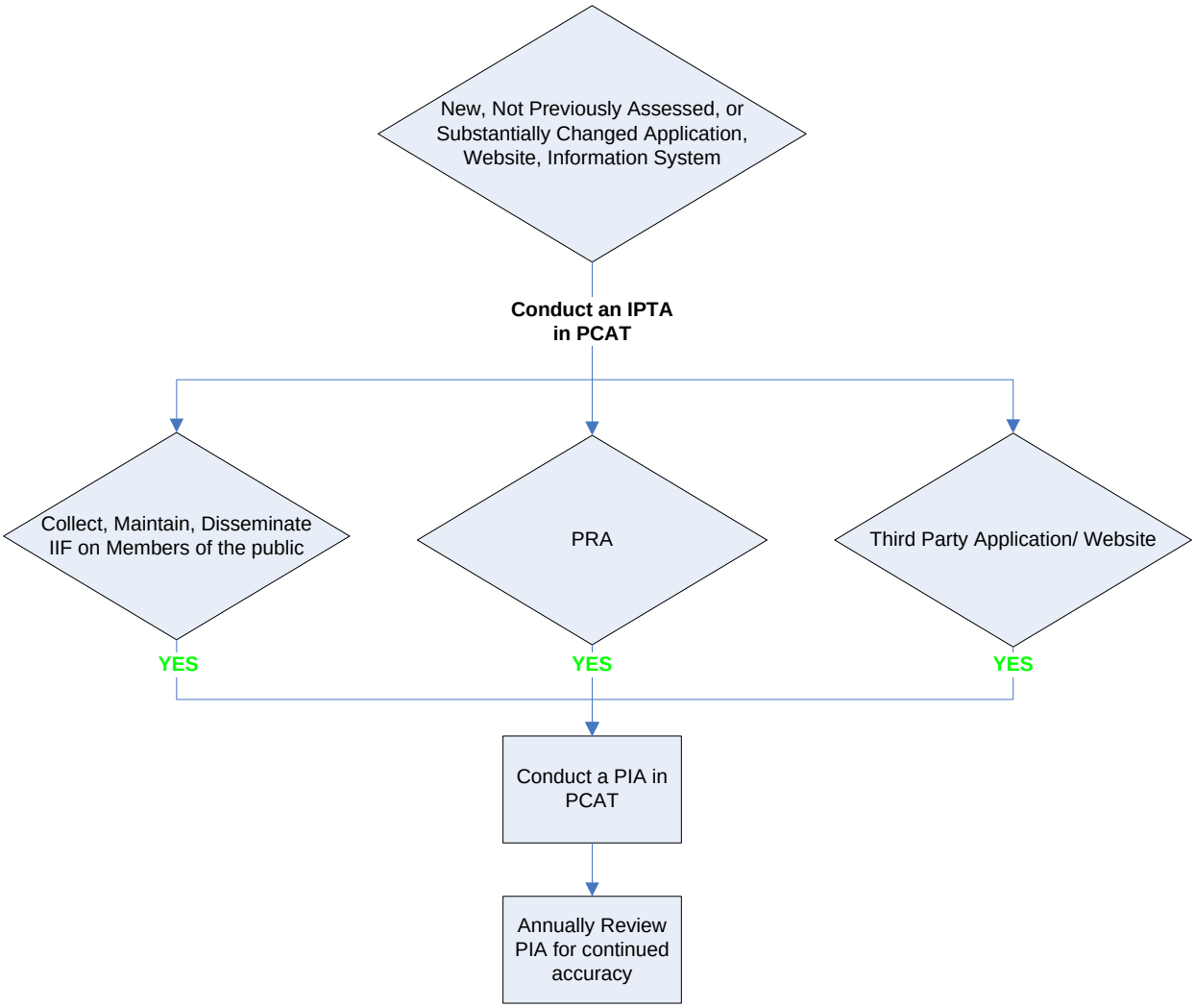


Figure 1: PIA Flow Chart

There is no exception for pilots. Any pilot application, website, or information system collecting PII or use of a third-party application/website must have a PIA prior to the pilot's launch.

6.3.2.1. Substantially Changed Application, Website, or Information System

System changes[11] to an application, website, or information system that prompt a re-evaluation of the IPTA and likely result in privacy risks that would require a full PIA include:

- CONVERSIONS - when converting paper-based records to electronic systems (or vice versa).
- ANONYMOUS TO NON-ANONYMOUS - when functions applied to an existing information collection change anonymous information into IIF.
- SIGNIFICANT SYSTEM MANAGEMENT CHANGES - when new uses of an existing IT system, including the application of new technologies, significantly change how IIF is managed within the system:
    - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
- SIGNIFICANT MERGING - when agencies adopt or alter business processes so that government databases holding IIF are merged, centralized, matched with other databases or otherwise significantly manipulated:
    - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns that were not previously an issue, or conversely, removing them.
- NEW PUBLIC ACCESS - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public.
- COMMERCIAL SOURCES - when agencies systematically incorporate IIF that was purchased or obtained from commercial or public sources into existing information systems databases. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement).
- NEW INTERAGENCY USES - when agencies work together on shared functions involving significant new uses or exchanges of IIF, such as the cross-cutting e-Government initiatives; in such cases, the lead agency should prepare the PIA.
    - For example, the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross-agency IT investment.
- INTERNAL FLOW OR COLLECTION - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of IIF:
    - For example, agencies that participate in e-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or e-Gov requirements. In most cases, the focus will be on integration of

[11] Non-Substantial Changes include minor changes to an application, website, or information system collection that do not create new privacy risks.

common processes and supporting data. Any business change that results in substantial new requirements for IIF could warrant examination of privacy issues.

- ALTERATION IN CHARACTER OF DATA - when new IIF is added to a collection, this raises the risks to individual privacy (for example, the addition of health or financial information).

6.3.2.2. Collect, Maintain, Disseminate IIF on Members of the Public

If NASA is electronically collecting, maintaining, or disseminating IIF from members of the public (excluding contractors) a PIA is required.

6.3.2.3. PRA

ISOs should work with the NASA PRA Clearance Officer in the OCIO to obtain OMB authorization to collect information under the PRA.[12]

6.3.2.4. Third-Party Application/Website

A third-party application/website is defined by OMB M-10-23 as "… 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."

NASA use of third-party applications and websites requires a PIA to ensure that privacy considerations are evaluated prior to the use of the application or website.

6.3.3. How to Conduct a PIA

The Privacy & CUI Assessment Tool (PCAT) assists the ISO in conducting the PIA. For each new application/website/information system the ISO should create the PIA in PCAT. See Appendix C for additional information on creating a PIA within PCAT.

6.3.3.1. Guidelines for Responding to PIA Questions

The following outlines basic guidelines for responding to PIA questions.

- ❑ REMEMBER THE AUDIENCE – The PIA responses within the comment fields should be written with the general public in mind. PIA's are published externally on the public-facing NASA website. Members of the public should be able to understand the activities and information being described in the PIA. Additionally, the PIA should be written in enough detail that the SAOP, NASA Privacy Programs Manager, and CPMs are able to analyze the privacy risks and mitigation steps. Great care should be exercised in use of abbreviations.
  - Note: Since the information is public, sensitive information such as specific details on security controls or implementation should not be provided. If the document needs to include information of a sensitive nature, contact the CPM.
- ❑ ERROR FREE – The PIA will be published for public consumption and should be free of spelling and grammatical errors.

[12] Note: ISOs are not required to conduct a new PIA when processing a PRA OMB Control Number renewal request. However, they should ensure that the PIA continues to accurately reflect the collection.

- ❑ WRITE OUT ACRONYMS – Make sure to spell out each acronym the first time it is used.
- ❑ USE PLAIN LANGUAGE – No abbreviations.
- ❑ USE SHORT AND SIMPLE SENTENCES – this will improve clarity and understanding.

6.3.4. When to Post a PIA

Publishing the PIA allows NASA to give the public notice of the analysis and promotes trust and transparency of NASA's collections of information from the public.

A PIA for a sensitive application, website, or information system may be exempted from the requirement to publically publish the PIA at the discretion of the NASA SAOP and/or Privacy Programs Manager. If an ISO wishes a PIA to be exempted from the publishing requirement, they should contact their CPM and the NASA Privacy Programs Manager with the justification.

6.3.5. When to Update a PIA

PIAs shall be updated when there has been a substantial change[13] made to the application, website, information system collecting PII.

- General Rule of Thumb for Updating a PIA: **Any noteworthy change to an application, website, information system, or the information being collected, requires a review and update of the PIA**.[14]

Noteworthy changes include new uses of an existing information system, including the application of new technologies, adding or removing of PII or IIF, significant change to how PII is managed within the application, website, or information system, or to the PII being collected.

6.3.6. Annually Review PIA for Continued Accuracy

On an annual basis, ISOs shall review the PIA for continued accuracy and make updates[15] to ensure members of the public are properly protected and notified of NASA's activities as it relates to their privacy.

7. Privacy Act SORNs

The SORN requirements are triggered by the collection of PII that is retrieved by a personal identifier. Per federal requirement and NASA policy, SORNs are published in the Federal Register for any electronic or non-electronic system of records that contains information on individuals routinely retrieved by personal identifiers. The Privacy Act requires agencies to publish a notice in the Federal Register for all SOR. A SOR is defined in the Privacy Act as "… a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. 167; 552a (a)(5).

[13] *See Section 6.3.2 Substantially Changed Application, Website, or Information System* for additional information.
[14] As stated previously, this is a responsibility of the ISO.
[15] If an update to the PIA is required, the ISO shall go into PCAT and archive the existing PIA. Once archived, PCAT will create a new document with the same name for the ISO to complete.

7.1.SORN Roles and Responsibilities

7.1.1.*The NASA SAOP shall*:

- Approve all SORN notices for publication in the Federal Register.

7.1.2.*The NASA Privacy Act Officer shall*:

- Review draft SORNs.
- Coordinate Agency review.
- Obtain NASA CIO's signature for submittal to the Federal Register for publication through the NASA Federal Register Liaison Officer.

7.1.3.*The CPM shall*:

- Assist the SOR System Manager in drafting the SORN.

7.1.4.*The SOR System Manager*[16] *shall*:

- Draft a SORN to be published in the Federal Register.

7.2.Record

According to the Privacy Act, a record is "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, [their] education, financial transactions, medical history, and criminal or employment history that contains [their] name, or other identifying particular assigned to the individual."

7.3.Name and Personal Identifier

In accordance with the Privacy Act, records that NASA maintains must be retrieved by a person's name or other PII (referred to as a personal identifier) to be a SOR. A personal identifier may include any of the following: an individual's name, address, e-mail address, telephone number, SSN, photograph, biometric information, or any other unique identifier that may be linked to that individual.

7.4.When does a System Require a SORN

A SORN is required when:

- Records are maintained by or on behalf of NASA containing information about individuals.
- Records are retrieved by an individual identifier.

7.4.1. Systems that do not qualify as SORs

A system that is not a SOR is one that only collects NASA employees' or contractors' names and work-related information. These systems do not qualify as SORs because the PII that is collected is public information that does not need to be protected – regardless of the data being retrieved by an individual's name. Additionally, a SORN is not required when records are not retrieved using a personal

[16] The SORN System Manager may be the IO, ISO, or another NASA individual. The SORN System Manager is system specific.

identifier. Although a system may be capable of retrieving the information using a personal identifier, if it does not regularly do so, then it is not a Privacy Act SOR.

7.5.Creating a New SORN vs. Amending an Existing SORN

See Appendix I of OMB Circular No. A-130, Federal Agency Responsibilities for Maintaining Records About Individuals for guidance on when a new SORN should be created vs. amended.

7.5.1. Government-wide SORNs

NASA SOR may be covered by an existing government-wide SORN.[17] An IO or ISO should work with the CPM to determine if a government-wide SORN covers their records.

7.6.SORN – Basic Elements

The basic elements of a SORN include:

- Name and location of the system
- Categories of individuals on whom records are maintained in the system
- Categories of records maintained in the system
- The authority for maintenance of the system
- Each routine use of records contained in the system, including the categories of users and the purpose of such use
- Policies and practices regarding the storage, retrievability, access controls, and retention and disposal of the records
- System manager(s) and address(es)
- Agency procedures whereby an individual may request information as to whether the system records pertain to him/her
- Agency procedures whereby an individual can request access to any record pertaining to him/her that is contained in the SOR and the process for contesting its content
- Categories of sources of records in the system

7.7.How to Develop a SORN

Step 1 – Draft a Federal Register Notice[18]

The SORN System Manager, with the assistance of the CPM, will draft a Federal Register notice of the system for the NASA CIO's signature. The CPM will coordinate Center legal review for Center-specific systems and submit the notice to the Privacy Act Officer for Agency-level review. See Appendix D for SORN format and content information.

Step 2 – Obtain Center Concurrences

The SORN System Manager shall obtain concurrence from the CPM and Office of the Chief Counsel.

[17] Government-wide SORNs begin with the identifier, GOVT-1, 2, etc.
[18] Once Phase 2 of PCAT is released SORN Development shall be conducted within PCAT.

Step 3 – Submit SORN to NASA Privacy Act Officer

The SORN System Manager shall submit the SORN to the NASA Privacy Act Officer.

Step 4 – Obtain NASA Privacy Act Officer Concurrence

The NASA Privacy Act Officer reviews the SORN and either concurs or sends it back to the SORN System Manager for revisions.

Step 5 – Obtain General Counsel Concurrences

The NASA Privacy Act Officer will ensure that the Office of the General Counsel has reviewed and concurs with the notice.

Step 6 – Obtain Agency Signoff

The NASA Privacy Act Officer will coordinate NASA CIO signature.

Step 7 – Provide Signed SORN to OCIO and NASA Federal Register Liaison Officer

The signed SORN will be provided by the NASA OCIO to the NASA Federal Register Liaison Officer for submittal to the Federal Register for publication.

Step 8 – Publish SORN

The NASA Federal Register Liaison Officer submits the SORN to the Federal Register for Publication.

7.7.1. Guidelines for Drafting a SORN

The following outlines the basic guidelines for drafting a SORN

- ❑ REMEMBER THE AUDIENCE – The SORN shall be written in a manner that allows the public to understand the SOR. Specifically, a member of the public should be able to understand the activities being described in the SORN.
- ❑ ERROR FREE – The SORN will be published for public consumption in the Federal Register and on NASA's external website; therefore, the SORN should be free of spelling and grammatical errors.
- ❑ WRITE OUT ACRONYMS – Make sure to spell out each acronym the first time it is used.
- ❑ USE PLAIN LANGUAGE
- ❑ USE SHORT AND SIMPLE SENTENCES – this will improve clarity and understanding.
- ❑ DEFINE TECHNICAL TERMS AND REFERENCES
- ❑ CITE LEGAL REFERENCES AND OTHER PREVIOUSLY PUBLISHED DOCUMENTS – this includes providing the complete name of reference documents.

8. Privacy Act (e) (3) Statements

SORN System Managers must ensure that individuals asked to supply information are presented with a Privacy Act Statement meeting the requirements outlined in 14 C.F.R. 1212.602 at the collection point for that information.

8.1. What goes in a Privacy Act Statement

Figure 2 addresses how to provide a Privacy Act statement under different collection circumstances.

Collection Method	Example	NASA Procedures to Provide a Privacy Notice
In Person	Interviews	Provide the notice in writing or orally. If notice is given orally, provide the notice before collecting data and include a note with the maintained information that notice was provided orally.
Hardcopy forms	• Clinic forms • Printed forms	Place the notice on the form near where data are collected or provide a separate Privacy Act Statement before collecting the data.
Telephone	Information collected for NASA visitor clearance	• Orally provide callers with a notice that meets the content requirements specified in this chapter. If the caller is using an automated system, when the caller is transferred to an option where information may be collected and maintained in an SOR, the system must deliver a statement that NASA has a privacy policy and must allow the caller to access the full content of the notice on the menu of options. • If a caller requests additional information, the call center agent will mail or e-mail a privacy notice to the caller.
Online	• Any Web-based form	• For employees or contractors, a privacy notice that meets the content requirements specified in this chapter must be available before data is collected. • For all others, provide a link to the NASA Web Privacy Policy located at http://www.nasa.gov on every public Web page and on major entry points.
E-mail		• If data may be collected as a result of an e-mail interaction and placed in an SOR, provide a privacy notice meeting the content requirements specified in this chapter. • Place the notice in the same e-mail that solicits data or include the notice in response to e-mails from the customer, employee, or other individual.

Figure 2: Privacy Act Statement Delivery Requirements

9. Computer Matching Agreements

At this time, NASA does not have any agreements that fall within the Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988. When NASA does have such agreements, the full process surrounding the Data Integrity Board will be provided.

Appendix A: Definitions

IIF	As outlined in NPR 1382, section 208(d) of the e-Gov act defines IIF as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." In accordance with OMB Memorandum M-03-22, IIF "is information in an IT system or online collection: (i) that directly identifies an individual (e.g. name, address, social security number or other identifying number or code, telephone number, e[-]mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."
Non-Sensitive PII	Non-Sensitive PII is information that is available in public sources the disclosure of which cannot reasonably be expected to result in personal harm.
PII	PII is defined in OMB Memorandum M-07-16 as "… referring to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." In accordance with OMB Memorandum M-10-23, "… [t]he definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information , could be used to identify an individual."
Privacy Act Record	According to the Privacy Act a record is "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, [their] education, financial transactions, medical history, and criminal or employment history that contains [their] name, or other identifying particular assigned to the individual."
Sensitive PII	Sensitive PII is a combination of PII elements, which if lost, compromised, or disclosed without authorization could be used to inflict substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII is any information or compilation of information, in electronic, non-electronic, or digital form that includes: (1) an individual's first and last name or first initial and last name in combination with any of the following data elements: a) Home address or telephone number [including personal cell phone numbers and personal e-mail addresses]; b) Mother's maiden name; c) Month, day, and year of birth; (2) A social security number (in whole or in part), driver's license number, passport number, or alien registration number or other government-issued unique identification number; (3) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation; (4) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; (5) Any combination of the following data elements: a) An individual's first and last name or first initial and last name; b) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or c) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.
Third-Party Application/Website	A third-party application/website is defined by OMB M-10-23 as "… 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."

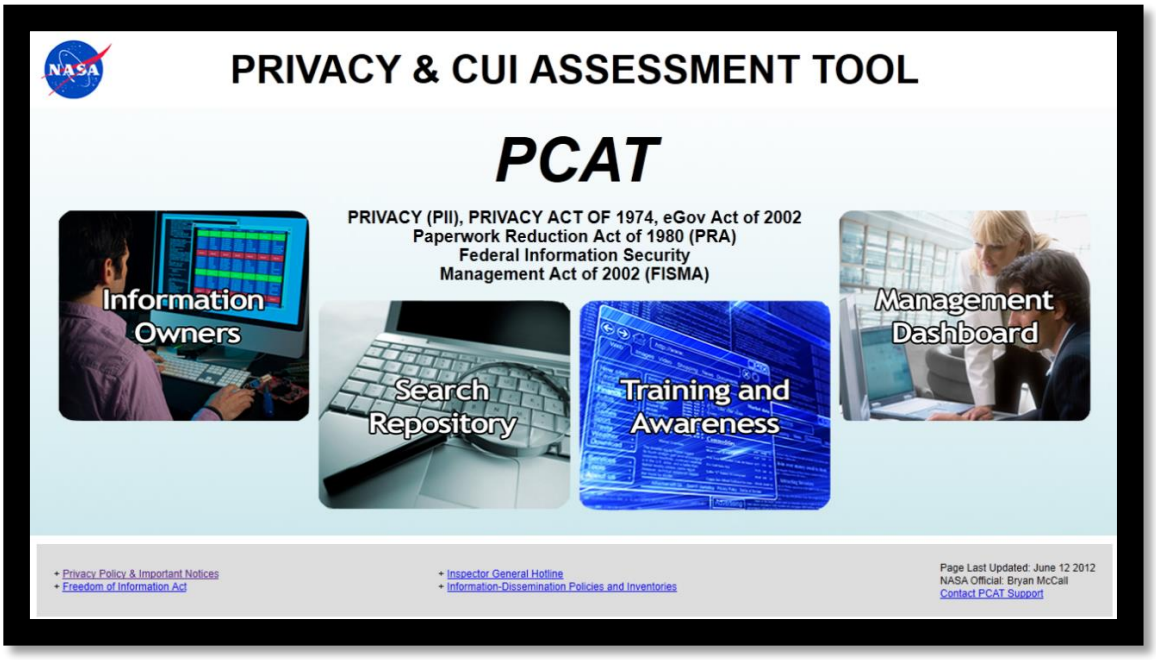
Appendix B: Acronyms

C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
COPPA	Children's Online Privacy Protection Act
CPM	Center Privacy Manager
CUI	Controlled Unclassified Information
DAAR	Privacy Act Disclosure Authorization And Accounting Record
e.g.	Exempli gratia
e-Gov	E-Government Act
FIPS	Federal Information Processing Standards
GRS	General Records Schedule
HBK	Handbook
IIF	Information in Identifiable Form
IO	Information Owner
IPTA	Initial Privacy Threshold Analysis
ISO	Information System Owner
ITS	Information Technology Security
ITSD	Information Technology Security Division
NASA	National Aeronautics and Space Administration
NF	NASA Form
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
NRRS	NASA Records Retention Schedule
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PCAT	Privacy & CUI Assessment Tool
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PRA	Paperwork Reduction Act
SBU	Sensitive But Unclassified Information
SOR	System of Records
SORN	System of Records Notice
SP	Special Publication

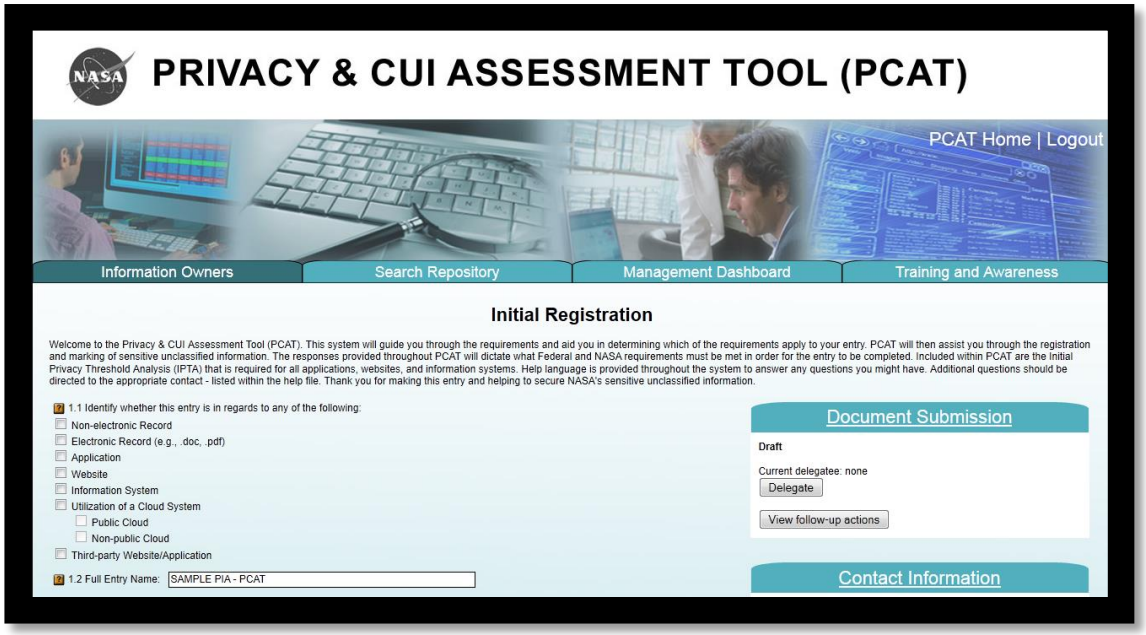
SSN	Social Security Number
U.S.C.	United States Code
UUPIC	Universal Uniform Personal Identification Code

Appendix C: Conducting a PIA in PCAT

To conduct a PIA within the PCAT go to: https://pcat.nasa.gov. The following entry screen will welcome you to PCAT. To create a new entry, select Information Owners (the upper left box).

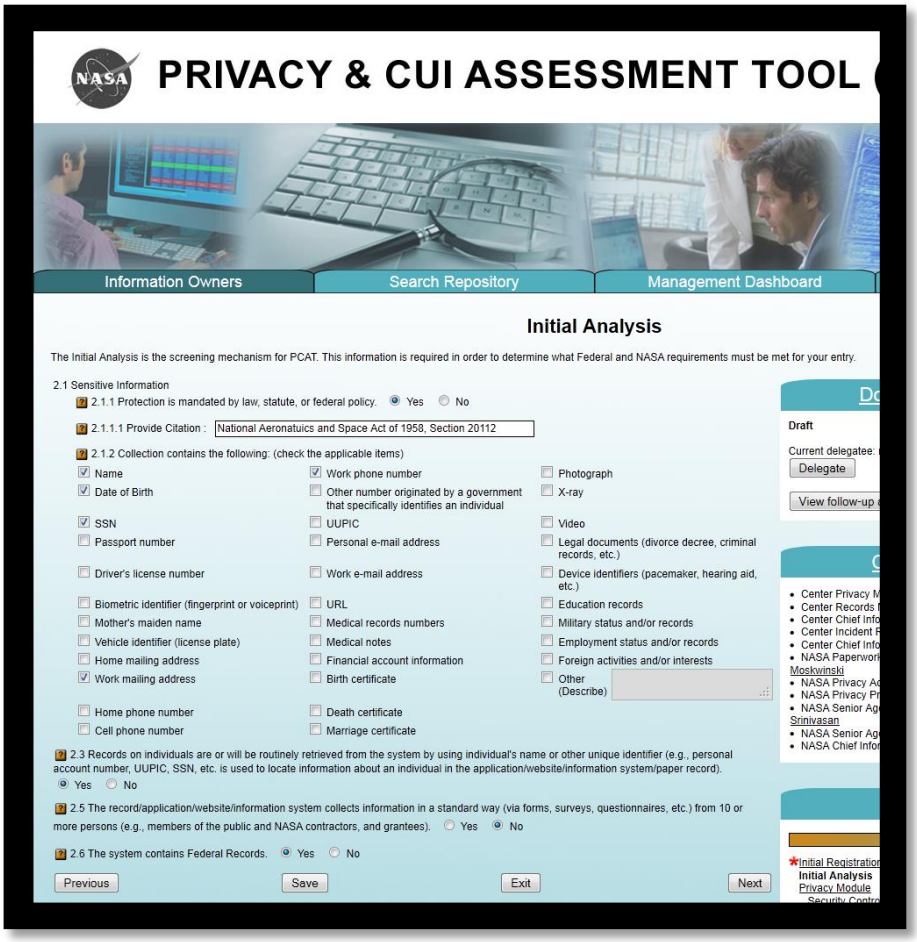


Once in the new entry screen, two initial sections are required – Initial Registration and Initial Analysis. To ensure the process is fast and pain free, be sure to review the help language for these pages by clicking on the orange help icon. Additionally, follow the PIA guidelines in 6.5.2.

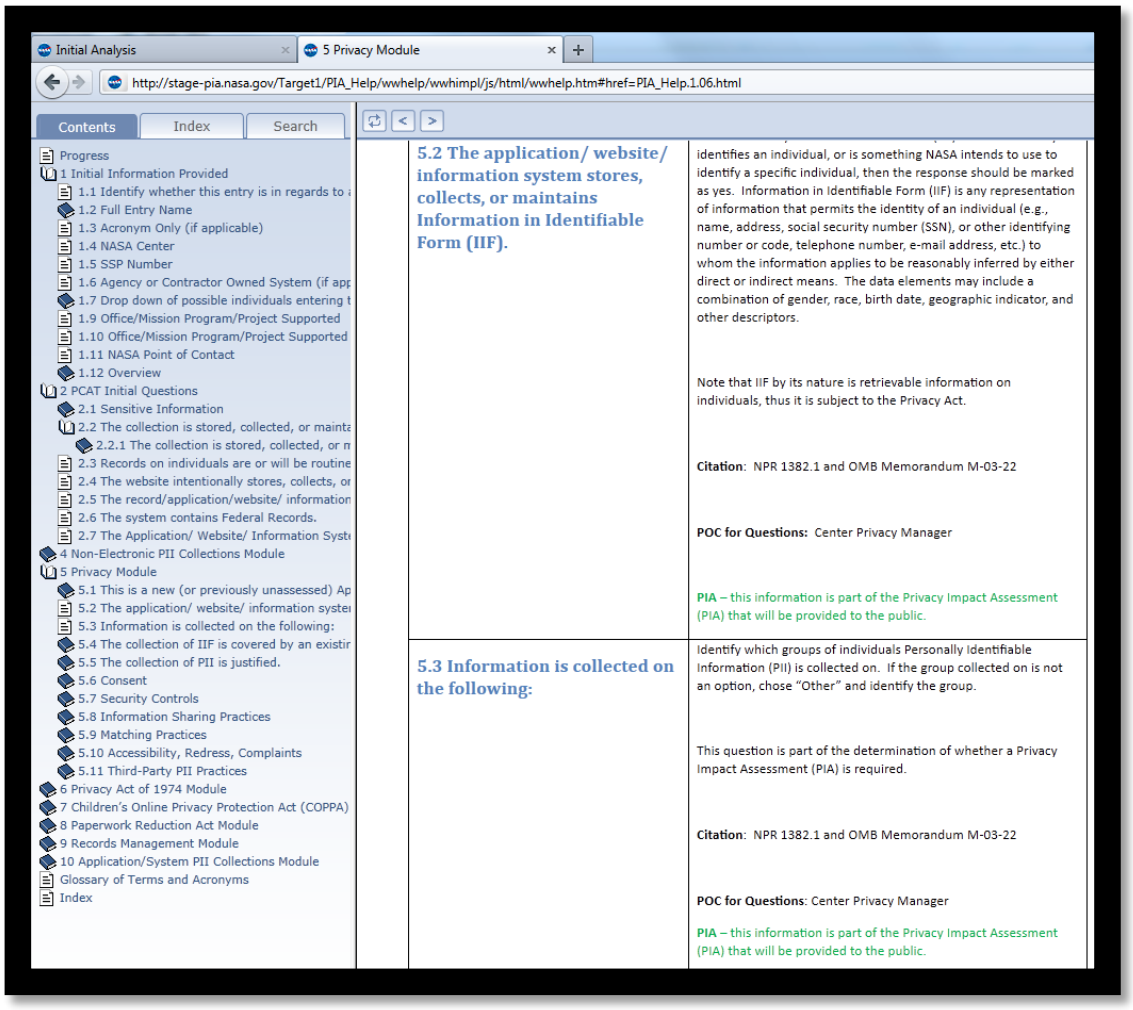


There is a progress bar in the bottom right of PCAT that tracks where you are in the process and whether you have any additional required responses.

As mentioned above, the final step to determing what modules are required is to complete the Initial Analysis. Make sure to mark all elements of PII in question 2.1.2.



Extensive help has been developed for each question within PCAT. The help language includes response guidance, question purpose, citation, and a point of contact for questions. Additionally, the help language identifies which questions and responses will be made available to the public in the PIA.



Appendix D: Format for a Federal Registry Notice - SORN

Below is the format for an SOR with sample verbiage and SORN preparation instructions in text boxes beneath the sample verbiage. The entire SORN document must be double-spaced. Initial SORN fields through "Supplementary Information" are standard for all Federal Register notices and should be completed in accordance with the Federal Register Document Drafting Handbook, 1998 edition.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Privacy Act of 1974; Privacy Act System of Records

AGENCY: National Aeronautics and Space Administration (NASA)

ACTION: Notice of Privacy Act system of records.

SUMMARY:

Sample Text: Each Federal agency is required by the Privacy Act of 1974 to publish a description of the systems of records it maintains containing personal information when a system is substantially revised, deleted, or created. In this notice, NASA provides the required information for a new system of records related to NASA's Integrated Financial Management Program (IFMP) Core Financial System. This new system will improve NASA's financial management systems in accordance with the requirements set forth in the Chief Financial Officers Act of 1990 and the Federal Financial Management Improvement Act of 1996.

DATES: Submit comments on or before 60 calendar days from the date of this publication.

ADDRESSES: (insert name), NASA Privacy Act Officer, Office of the Chief Information Officer, NASA Headquarters, 300 E Street SW., Washington, DC 20546– 0001, 202-358-4787, NASA PAOfficer@nasa.gov.

FOR FURTHER INFORMATION CONTACT: NASA Privacy Act Officer, (insert name), 202-358-4787, NASA-PAOfficer@nasa.gov.

SUPPLEMENTARY INFORMATION: Pursuant to Section 208 of the E-Government Act of 2002, NASA has conducted a Privacy Impact Assessment (PIA) for this system. A copy of the PIA can be obtained by contacting the NASA Privacy Act Officer at the address listed above. Authorization as an Information Collection under the Paperwork Reduction Act is being sought from OMB and will be noticed as a separate submission.

NASA ##XXXX:

Note: This is a number assigned by the NASA Privacy Act Officer.

SYSTEM NAME:

Note: The name is descriptive of the records maintained in the system or the individuals on whom the records are maintained.

SECURITY CLASSIFICATION:

The security classification describes any special control classification for the system. If there is none then it will state none. Note that most NASA SORNs do not have security classifications.

Sample Text: This system is categorized in accordance with OMB Circular A–11 as a Special Management Attention Major Information System. A security plan for this system has been established in accordance with OMB Circular A–130, Management of Federal Information Resources.

SYSTEM LOCATION:

System Location requires the specific identification of each address or location at which records are maintained. For a system with many locations, the list of addresses and locations may be included in an Appendix A. For example, if records are maintained in multiple NASA Centers, rather than one centralized IT system, this section may read: "Locations 1 through 9 and Locations 11, 12, and 14 as set forth in Appendix A."

Note that Appendix A is a standard appendix to all NASA SORNs, and lists all applicable NASA installations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This section requires the identification of each category of individuals covered by the system. This identification must be specific and stated in a manner clearly understood by the general public. One example is: "All non-U.S. citizens, to include Lawful Permanent Residents, seeking access to NASA facilities, laboratories, contractor sites, or NASA-sponsored events for unclassified purposes to include employees of NASA or NASA contractors; prospective NASA or NASA contractor employees; employees of other U.S. government agencies or their contractors."

CATEGORIES OF RECORDS IN THE SYSTEM:

This section requires specific identification of each type of record or information maintained in the system. This must be an all-inclusive list that is clear and understandable to the general public. Acronyms, abbreviations, and references to public laws and regulations will be avoided. If there are many data fields, list larger groupings that comprehensively incorporate the nature of all the smaller detailed fields maintained. The language from the retired SORN for the NASA Foreign National Management System serves as an example below: "Records in this system include information about the individuals seeking access to NASA resources. Information about an individual may include, but is not limited to: name, home address, place of birth and citizenship, U.S. visitor/travel document numbers, employment information, tax identification numbers (social security number), and reason and length of proposed NASA access."

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This section requires the identification of the specific statutory provision(s) that authorizes the solicitation and maintenance of the information in the system of records. The authority must be statutory, not regulatory; that is, it must cite the United States Code or a public law rather than the Code of Federal Regulations.

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

These are brief, concise, clear statements of the disclosures of the information maintained in the SOR. The term "routine use" means the disclosure of a record or information from the system outside the Agency for a purpose that is compatible with the purpose for which it was collected. The statement of a routine use must identify, as specifically as possible, the information that may be disclosed under the routine use, to whom the record(s) or information may be given, and the purpose(s) or use(s) for which information may be disclosed. Routine use statements will be numbered sequentially. Note: This paragraph is the most critical portion of the notice. If there is no routine use statement or the statement is not written precisely, NASA may not be able to disclose information from the SOR when it wishes to initiate a disclosure or when disclosure is requested by a third party.

Specify, by reference of the numbers from Appendix B (standard appendix for all NASA SORNS) any "Standard Routine Uses" that apply to this system, the appendix to NASA's comprehensive listing of SORs and attached to this sample SORN. This was already published in the Federal Register as "Appendix B" and is always referenced as such.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

This section requires a description of the medium and/or manner in which the records are maintained, such as microfilm, magnetic tape, on server, CD, or paper file folders. If this varies by location, such as field Centers, explain the storage at each location.

RETRIEVABILITY:

This section requires an explanation by what data field(s) records are indexed and routinely retrieved.

SAFEGUARDS:

This section requires a brief description of the measures taken to prevent unauthorized access and disclosure of records, such as physical security, personnel screening, or technical safeguards. Include such safeguards as those for natural disasters, such as tornadoes, and backup and offsite storage and operations if the site is damaged or destroyed, as well as the estimated time to return the system to operation. A statement such as "Standard security procedures will be followed" is not sufficient. An approved IT Security Plan or mentioning that “analyses of the system were conducted as required by Federal Information Processing Standard (FIPS) 199 and applicable security controls implemented in accordance with FIPS 853,” are additional evidence that proper security measures have been evaluated and implemented.

RETENTION AND DISPOSAL:

This section requires the approved disposition authority under which the records are retained and archived or disposed of to be provided. This must be either a specific NRRS item such as “Schedule 1, Item 35” or a GRS item published by the National Archives such as “GRS 14, Item 24(a).” This Notice will not be approved by the NASA Privacy Act Officer for publication unless a proper retention schedule is either approved by the National Archives and Records Administration (NARA) or, at a minimum, drafted for submission for NARA’s approval. Work with your Center Records Manager to identify a proper schedule item or to develop one for submission for approval by the Archivist of the United States.

SYSTEM MANAGER(S) AND ADDRESS:

This section requires the title, office symbol, and address of the NASA official(s) responsible for the policies and practices governing the System of Records (SOR) to be provided. Do not include the individual's name. Identify this individual as the System Manager; the term "System Manager" is prescribed by the Privacy Act. If system records are maintained in physically separate locations, list all managers as Subsystems Managers and provide their addresses. Locations and the addresses may be listed by a reference to Appendix A. For example, for all health records maintained by NASA: "Director, NASA Occupational Health Office, Location 1. Subsystem Managers: Chief Engineer, Location 2; Assistant Director for Life Sciences, Space and Life Sciences Directorate, Location 5; Director, Biomedical Operations Office, Location 6; Director, Management Services Office, Location 9. Locations are as set forth in Appendix A.

Sample Text: AD04/Manager of the IFMP Competency Center, George C. Marshall Space Flight Center, National Aeronautics and Space Administration, Marshall Space Flight Center, AL 35812

NOTIFICATION PROCEDURE:

This section requires the address(es) of the NASA office(s) to which inquiries must be sent and address(es) of the location(s) at which the individual may present a request as to whether a system contains records pertaining to himself/ herself to be provided. Include any identifying information that an individual is required to provide to permit the Agency to determine whether a system contains a record about the individual.

Sample Text: Individuals interested in inquiring about their records should notify the System Manager at the address given above.

RECORD ACCESS PROCEDURE:

This section requires the name(s) and address(es) of the NASA office(s) to which the individual may go or write to obtain information from his/her record to be provided. This information is for the individual who already knows that a system contains information about him/her.

Sample Text: Individuals who wish to gain access to their records should submit their request in writing to the System Manager at the address given above.

CONTESTING RECORD PROCEDURES:

This section should refer the reader to 14 CFR Part 1212 for instructions on how to contest the records or appeal decisions contained in NASA SORs.

Sample Text: The NASA regulations governing access to records and procedures for contesting the contents and for appealing initial determinations are set forth in 14 CFR Part 1212.

RECORD SOURCE CATEGORIES:

This section requires the description, as specifically as possible, of the source of the records or information in the system. For example, did the information come from an individual, employee, or other source? To the greatest extent possible, this should be limited to the source of the information.

Sample Text: The information is received by the IFMP Core Financial System through an electronic interface from the NASA Personnel Payroll System (NPPS). In certain circumstances, updates to this information may be submitted by NASA employees and recorded directly into the IFMP Core Financial System.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

This section requires the specific provisions of the Privacy Act from which the system is being exempted and the specific reason(s) for exemption. This element is optional. This element is only permissible if NASA regulations specifically state the system is exempt. There currently are two systems with exemptions – Security records and Inspector General Records are exempt as they are law enforcement related.

(insert name)
Chief Information Officer

APPENDIX A

LOCATION NUMBERS AND MAILING ADDRESSES OF NASA INSTALLATIONS AT WHICH RECORDS ARE LOCATED

Location 1. NASA Headquarters, National Aeronautics and Space Administration Washington, DC 20546-0001

Location 2. Ames Research Center, National Aeronautics and Space Administration, Moffett Field, CA 94035-1000

Location 3. Dryden Flight Research Center, National Aeronautics and Space Administration, PO Box 273, Edwards, CA 93523-0273

Location 4. Goddard Space Flight Center, National Aeronautics and Space Administration, Greenbelt, MD 20771-0001

Location 5. Lyndon B. Johnson Space Center, National Aeronautics and Space Administration, Houston, TX 77058-3696

Location 6. John F. Kennedy Space Center, National Aeronautics and Space Administration, Kennedy Space Center, FL 32899-0001

Location 7. Langley Research Center, National Aeronautics and Space Administration, Hampton, VA 23681-2199

Location 8. John H. Glenn Research Center at Lewis Field, National Aeronautics and Space Administration, 21000 Brookpark Road, Cleveland, OH 44135-3191

Location 9. George C. Marshall Space Flight Center, National Aeronautics and Space Administration, Marshall Space Flight Center, AL 35812-0001

Location 10. HQ NASA Management Office-JPL, National Aeronautics and Space Administration, 4800 Oak Grove Drive, Pasadena, CA 91109-8099

Location 11. John C. Stennis Space Center, National Aeronautics and Space Administration, Stennis Space Center, MS 39529-6000

Location 12. JSC White Sands Test Facility, National Aeronautics and Space Administration, PO Drawer MM, Las Cruces, NM 88004-0020

Location 13. GRC Plum Brook Station, National Aeronautics and Space Administration, Sandusky, OH 44870

Location 14. MSFC Michoud Assembly Facility, National Aeronautics and Space Administration, PO Box 29300, New Orleans, LA 70189

Location 15. NASA Independent Verification and Validation Facility (NASA IV&V), 100 University Drive, Fairmont, WV 26554

Location 16. Edison Post of Duty, c/o DCIS, PO 1054, Edison, NJ
08818

Location 17. Western Field Office, Glenn Anderson Federal Building, 501 West Ocean Blvd., Long Beach, CA 90802-4222

APPENDIX B

STANDARD ROUTINE USES—NASA

The following routine uses of information contained in SORs, subject to the Privacy Act of 1974, are standard for many NASA systems. They are cited by reference in the paragraph "Routine uses of records maintained in the system, including categories of users and the purpose of such uses" of the Federal Register Notice on those systems to which they apply.

Standard Routine Use No. 1—LAW ENFORCEMENT—In the event this system of 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, the relevant records in the SOR may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

Standard Routine Use No. 2—DISCLOSURE WHEN REQUESTING INFORMATION–A record from this SOR may be disclosed as a "routine use" to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

Standard Routine Use No. 3—DISCLOSURE OF REQUESTED INFORMATION–A record from this SOR may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

Standard Routine Use No. 4—COURT OR OTHER FORMAL PROCEEDINGS–In the event there is a pending court or formal administrative proceeding, any records that are relevant to the proceeding may be disclosed to the Department of Justice or other agency for purposes of representing the Government, or in the course of presenting evidence, or they may be produced to parties or counsel involved in the proceeding in the course of pretrial discovery.