



| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

NASA Procedural Requirements

NPR 1382.1
Effective Date: August 10,
2007
Expiration Date: April 28, 2013

COMPLIANCE IS MANDATORY

NASA Privacy Procedural

Responsible Office: Office of the Chief Information Officer

Table of Contents

Change History

Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents
- P.5 Measurement/Verification
- P.6 Cancellation

Chapter 1. Privacy Requirements Overview

- 1.1 Information on Individuals
- 1.2 Governing Statutes
- 1.3 Complying with Statutory Requirements
- 1.4 Required Activities by Life-Cycle Phases

Chapter 2. Safeguarding Electronic PII

- 2.1 General
- 2.2 Mobile Devices
- 2.3 Remote Access
- 2.4 Data Transport and Remote Storage
- 2.5 Personnel Training and Security Awareness
- 2.6 Extracted Data

Chapter 3. Privacy Impact Assessments

- 3.1 General

- 3.2 When to Conduct an IPTA
- 3.3 When to Conduct a PIA
- 3.4 When PIAs are Not Required
- 3.5 Conducting a PIA
- 3.6 Review, Approval, and Publication of a PIA
- 3.7 Relationship to Requirements under the Paperwork Reduction Act
- 3.8 Relationship to Requirements under the Privacy Act

Chapter 4. NASA Web Site Privacy

- 4.1 General
- 3.2 Privacy Policy on NASA Web Sites
- 4.3 Collecting PII

Chapter 5. Privacy Act Systems of Records

- 5.1 General
- 5.2 Creating or Modifying a Privacy Act SOR
- 5.3 Collecting Information for a Privacy Act SOR
- 5.4 Using Privacy Act Records
- 5.5 Maintaining and Disposing of Privacy Act Records
- 5.6 Contractors and Systems of Records

- Appendix A. Glossary
- Appendix B. Acronym List
- Appendix C. Tracking Waiver Template
- Appendix D. References
- Appendix E. Privacy Actions by Information Stage
- Appendix F. Guidance for Privacy Impact Assessments
- Appendix G. Web Privacy Guidance
- Appendix H. Privacy Act Guidance
- Appendix I. Measurement/Verification Matrix

Change History

NPR 1382.1, NASA Privacy Procedural Requirements

Chg #	Office/Center	Date	Distribution/Comments
-------	---------------	------	-----------------------

Preface

P.1 Purpose

This document sets forth the procedural requirements for protecting the privacy of personal information, regardless of format, that is collected, used, maintained, and disseminated by the National Aeronautics and Space Administration (NASA) through meeting statutory requirements for these processes. These requirements address when and how to conduct a Privacy Impact Assessment (PIA), the management of information in Privacy Act Systems of Records (SORs), and privacy concerns with Web pages.

This NASA Procedural Requirement (NPR) is based on Federal requirements. State requirements should be followed where applicable and more stringent.

P.2 Applicability

This NPR is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to the NASA Jet Propulsion Laboratory (JPL), other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

P.3 Authority

- a. National Aeronautics and Space Act of 1958, as amended, 42 U.S.C. ° 2473(c) (l).
- b. E-Government Act of 2002 (E-Gov Act), as amended, 44 U.S.C. °° 101 et seq.
- c. Privacy Act of 1974, as amended, 5 U.S.C. ° 552a.
- d. NASA Policy Directive (NPD) 1382.17, NASA Privacy Policy.

P.4 Applicable Documents

- a. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. ° 3535.
- b. Paperwork Reduction Act of 1995 (PRA), as amended, 44 U.S.C. °° 3501 et seq.
- c. Children's Online Privacy Protection Act of 1998 (COPPA), as amended, 15 U.S.C. °° 6501 et seq.
- d. NASA Privacy Act Regulations, 14 Code of Federal Regulations (CFR) Part 1212.
- e. Clinger-Cohen Act of 1996, 40 U.S.C. 11103.
- f. The Government Performance and Results Act (GPRA) of 1993, as amended, 31 U.S.C. °° 1101-1119, 9703-9704.
- g. The Federal Acquisition Regulations (FAR), 48 CFR Parts 1-99.
- h. NPR 1441.1, NASA Records Retention Schedules.
- i. NPR 1600.1, NASA Security Program Procedural Requirements.

- j. NPD 2540.1 Personal Use of Government Equipment including Information Technology.
- k. NPR 2810.1, Security of Information Technology.
- l. NPR 2830.1, NASA Enterprise Architecture Procedures.
- m. Federal Information Processing Standards (FIPS) Uniform Resource Locator (URL):
<http://csrc.nist.gov/publications/fips/index.html>.
- n. National Institute of Standards and Technology (NIST) Special Publications (SPs) 800 Series.
- o. Federal Register Document Drafting Handbook, 1998.

P.5 Measurement/Verification

Measurement/Verification Matrix is included as Appendix I.

P.6 Cancellation

None.

/S/

Jonathan Q. Pettus
Chief Information Officer

Chapter 1. Privacy Requirements Overview

1.1 Information on Individuals

1.1.1 NASA is committed to protecting the privacy of individuals from and about whom it collects, maintains, uses, and disseminates information. Such information is referred to by different labels in different statutes and Office of Management and Budget (OMB) instructions to agencies, including "personally identifiable information" (PII), Privacy Act records, and "information in identifiable form" (IIF).

1.1.2 These terms are defined in Appendix A of this document. The definitions of PII and Privacy Act records are nearly identical, and all three terms are often used interchangeably by OMB. However, PII is used most predominately; therefore, this NPR defaults to PII with the exception of using "IIF" with respect to PIA requirements and "records" with respect to SORs, in accordance with governing statutes. As used in this document, PII excludes strictly business contact information (such as work e-mail address, office location, and office telephone number) for NASA employees and contractors.

1.2 Governing Statutes

1.2.1 The Federal laws that impact NASA's collection and management of PII include the Privacy Act of 1974 (hereinafter referred to as the Privacy Act), the Children's Online Privacy Protection Act of 1998 (COPPA), the E-Government Act of 2002 (E Gov Act), the Federal Information Security Management Act of 2002 (FISMA), and the Paperwork Reduction Act of 1995 (PRA).

1.2.2 This section provides a summary of each of these laws and its basic privacy requirements, as related to NASA's management of information. The specifics of their requirements and responsibilities for compliance are elaborated in subsequent chapters.

1.2.2.1 The Privacy Act of 1974.

The Privacy Act sets forth extensive requirements for the management of personal information maintained in any format on individuals where such information is retrieved by a name or personal identifier unique to the individual. Chapter 5 fully elaborates Privacy Act requirements; however, some of the most basic Privacy Act requirements of system managers/owners are that they must:

- a. Publish SOR Notices (SORNs) in the Federal Register.
- b. Provide specific notification to individuals at the time of information collection.

1.2.2.2 Children's Online Privacy Protection Act of 1998.

The COPPA regulates the Agency's operation of Web site or online services directed to children under age 13 when the Web site or service collects personal information from children. Full descriptions of COPPA requirements are contained in Chapter 4. However, the basic requirements levied for NASA Web sites or services concern site owner or operator responsibilities with respect to notice of information collection practices, verifiable parental consent, and access, including:

- a. Providing notice concerning what information is collected from children by the operator, how the information will be used, and the operator's disclosure practices.
- b. Obtaining verifiable parental approval for the collection, use, or disclosure of information from

children.

c. Providing a process for parental review of information collected from the child, an opportunity for parental refusal to permit the operator's future use of the information or future collection of information, and a means for the parent to obtain the personal information collected from the child.

1.2.2.3 Paperwork Reduction Act of 1995.

The PRA regulates the burden that agencies place on members of the public in collecting information from them, but is addressed in this document only as it relates to privacy. OMB authorization must be obtained when NASA collects information from 10 or more members of the public through standardized fields, whether via survey, Web-enabled forms, or other requirements of information provision, regardless of format or whether provision of the information is voluntary. In contrast to the E-Gov Act, which excludes contractors and partners as members of the public, the PRA includes contractors as "members of the public," with the general exception of when they are providing the information in carrying out a specific task under the contract. While the PRA is concerned with the collection of any type of information, it is relevant to these privacy procedural requirements only when NASA seeks collection of IIF from the public.

1.2.2.4 E-Government Act of 2002.

The E-Gov Act is addressed in this document only as it relates to privacy issues. In this respect, the E-Gov Act reinforces existing statutory privacy provisions and adds new requirements to ensure sufficient protections for the privacy of personal information as agencies implement electronic government.

a. Title III of the E-Gov Act, entitled "Federal Information Security Management Act" (FISMA), provides for development and maintenance of minimum controls required to protect Federal information and information systems. It also authorizes OMB and the NIST, under the U.S. Commerce Department, to define what is meant by "minimum controls required." Briefly, the following are requirements specifically related to PII: (1) Designation of all systems containing PII information to be categorized, at a minimum, as "Moderate," as defined in NIST FIPS 199. All requirements for "Moderate" systems identified within NPR 2810.1, Security of Information Technology, are to be met and will be certified as part of the NASA Certification and Accreditation (C&A) process.

(2) Implementation of specific controls for systems containing PII.

b. Specific new privacy requirements in Section 208 of the E-Gov Act and OMB guidance for implementing them are summarized below and detailed in the following chapters:

(1) PIAs must be conducted and made publicly available for all information technology (IT) systems, including Web sites, which collect and/or maintain IIF on members of the public. The phrase "members of the public," under the E-Gov Act, excludes Government personnel, contractors, and partners. Detailed requirements for conducting PIAs are provided in Chapter 3.

(2) Agencies are prohibited from using persistent tracking technology or "persistent cookies" on public Web sites. Web content managers must seek the approval of the NASA Chief Information Officer (CIO) to use persistent tracking technology under certain circumstances described, along with the approval process, in Chapter 4.

(3) Requirements are prescribed for Web privacy policy placement, clarity, and format, as well as Web privacy policy content regarding public consent to the collection and sharing of information and their rights under privacy laws. These Web-related requirements are elaborated in section 4.2.

1.3 Complying with Statutory Requirements

1.3.1 The three facets that determine which requirements apply in NASA processes are:

- a. How information is obtained or maintained.
- b. From or on whom the information is collected or maintained.
- c. How the information is retrieved.

1.3.2 Employee failure to comply with requirements in this document carries sanctions including reprimand, suspension, removal, fines, or other actions in accordance with applicable laws and Agency disciplinary policy.

1.4 Required Activities by Life-cycle Phases

A summary of the various actions necessary for the planning and management of PII through different phases in the life cycle of information itself is provided in Appendix E.

Chapter 2. Safeguarding Electronic PII

2.1 General

There are common and essential requirements across the Agency for safeguarding all PII in digital form. All PII must be handled and protected as Sensitive But Unclassified (SBU) information in accordance with NPR 1600.1, NASA Security Program Procedural Requirements. There are several specific common requirements for protecting and monitoring the movement of digital PII.

2.2 Mobile Devices

2.2.1 Any PII on mobile computers/devices shall, at a minimum, be encrypted by users with Entrust or native encryption in Microsoft and Apple operating systems or any other NASA CIO-approved encryption solution.

2.2.2 A "time-out" function requiring user reauthentication after a maximum of 30 minutes of inactivity shall be employed by users for mobile devices or with remote access.

2.2.3 When any mobile storage device contains PII, users shall label the device, at a minimum, with "NASA Privacy Information; Protect Accordingly."

2.3 Data Access

2.3.1 System owners shall ensure that access to PII on their systems is only accomplished by users via two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

2.3.2 Access to PII shall use a "time-out" function that requires user reauthentication after 30 minutes of inactivity.

2.4 Data Transmission

PII data must be protected during transmission. PII data will be encrypted using FIPS 140 2 compliant encryption methodology (e.g., Secure Socket Layer (SSL) or Internet Protocol Security (IPsec)).

2.5 Data Transport and Remote Storage

Employees shall only remove PII from NASA premises or download and store PII remotely under conditions prescribed in NPR 1600.1.

2.6 Personnel Training and Security Awareness

NASA supervisors shall ensure that their employees who have access to PII are adequately trained and supervised in their responsibilities with regard to safeguarding PII and protecting it from unauthorized disclosure.

2.7 Extracted Data

System owners shall ensure that all computer-readable data extracts from databases containing PII are logged and verified, including information on whether the extracted data have been erased within 90 days or that the data's use is still required.

Chapter 3. Privacy Impact Assessments

3.1 General

Because the E-Gov Act prescribes PIAs for IT systems relative to their collection and/or maintenance of IIF, this chapter uses the term IIF for discussing information collected on individuals.

3.1.1 NASA has developed an assessment tool called the Information and Privacy Threshold Analysis (IPTA) to evaluate the nature of the information to be collected and maintained in applications and IT systems. Answers to the IPTA questions allow the determination of what actions must be taken to comply with applicable statutes, including the completion of a PIA.

3.1.2 A PIA, required by the E-Gov Act as well as by NIST SP 800-53 for IT Security C&A, is a process through which system owners analyze how information is managed to ensure that its handling conforms to applicable statutory, regulatory, and policy requirements regarding privacy and to determine the risks and effects of collecting, maintaining, and disseminating IIF. In addition, the PIA examines and documents the evaluation of protections and alternative processes for handling information to mitigate potential privacy risks.

3.2 When to Conduct an IPTA

3.2.1 Prior to application development, procurement, or modification, all application owners shall complete the IPTA that is available through the NASA Privacy Web site located at http://insidenasa.nasa.gov/ocio/information/info_privacy/index.html.

3.2.2 Prior to system development, procurement, or modification, all system owners shall complete, at a minimum, the IPTA that is available through the NASA Privacy Web site. The results of the IPTA responses will indicate whether the application owner and/or system owner must complete a PIA.

3.2.3 If the completed IPTA for a system does not indicate the need for a PIA, the IT system owner shall retain the record copy, submit a copy of the completed IPTA(s) for the IT Security C&A process, and provide information copies to the Center Privacy Act Manager (PAM) and Center Records Manager.

3.3 When to Conduct a PIA

Prior to system development, procurement, or modification, system owners shall, in collaboration with their application owners and NASA cognizant officials, conduct PIAs for all new systems or significantly modified systems under the following circumstances:

- a. When the system will collect, maintain, or disseminate IIF from or about members of the public, excluding contractors and partners.
- b. When initiating a new electronic collection of IIF for 10 or more persons (excluding agencies, instrumentalities, or employees of the Federal Government) that is subject to the PRA.
- c. When the system will contain IIF or PII on any individuals, and the system requires an enterprise architecture (EA) review as prescribed by NPR 2830.1, NASA Enterprise Architecture Procedures.

d. When existing systems meeting one of the above criteria are changed such that the change creates new privacy risks. Examples of such changes are provided in Appendix F.

3.4 When PIAs are not Required

A PIA is not required if any of the following circumstances exist:

- a. The system has not undergone significant revision since April 2003 when the E-Gov Act was enacted.
- b. A system has been previously assessed under an evaluation similar to a PIA.
- c. The system's privacy issues are unchanged. Examples of such instances are provided in Appendix F.

3.5 Conducting a PIA

Discussion of how to conduct a PIA is contained in Appendix F.

3.6 Review, Approval, and Publication of a PIA

3.6.1 System owners shall submit the fully completed PIA worksheet and summary to the NASA Privacy Act Officer through the Center PAM and Center CIO.

3.6.2 The NASA Privacy Act Officer shall review fully completed PIA worksheets and summaries.

3.6.3 The NASA CIO shall approve all fully completed PIAs and make publicly available through the NASA privacy Web site those PIAs that concern applications/systems collecting or maintaining IIF on members of the public, retaining the record copy and providing a copy of the approved PIA to the Center CIO for the system owner's files.

3.6.4 The NASA CIO may determine not to make the PIA document or summary publicly available when publication would raise security concerns, reveal classified (i.e., national security) information, or disclose sensitive information (e.g., potentially damaging to national interest, law enforcement effort, or competitive business interest).

3.7 Relationship to Requirements under the PRA

Numerous similarities exist between information required in a PIA and that required for application for PRA authorization. The relationship between the two processes and steps to minimize duplicative effort is addressed in Appendix F.

3.8 Relationship to Requirements under the Privacy Act

There are numerous similarities between information required in a PIA and that required for Privacy Act SORN. Measures to minimize duplicative effort are addressed in Appendix F.

Chapter 4. NASA Web Site Privacy

4.1 General

4.1.1 This chapter establishes procedures for ensuring the privacy and protection of PII on, or collected by, NASA Web sites.

4.1.2 Web sites that are designed to accomplish a NASA function and that are operated under a contract are, in effect, deemed to be maintained by the Agency and are subject to these procedural requirements.

4.2 Web Site Assessment

The Responsible NASA Official (RNO) for each NASA Web site shall complete an IPTA as prescribed in Chapter 3, the results of which will enable determination of the applicability of the remaining requirements of this chapter.

4.3 Privacy Policy on NASA Web Sites

4.3.1 The "NASA Web Privacy Policy and Important Notices" (referred to hereafter as "NASA Web Privacy Policy") is available through the NASA Office of the CIO (OCIO) Web site. The NASA CIO shall ensure that the Web Privacy Policy:

- a. Informs visitors as to whether their provision of requested information is voluntary.
- b. Informs visitors on how to grant consent for the use of voluntarily provided information.
- c. Informs visitors on how to grant consent for NASA to use the information that the Web site collects via required fields for other than statutorily mandated uses or authorized routine uses under the Privacy Act.
- d. Notifies Web site visitors of their rights under the Privacy Act, where appropriate (see section 5.3.2).
- e. Specifies what information NASA collects automatically (e.g., user's internet protocol (IP) address, location, and time of visit) and identifies the use for which it is collected (i.e., site management or security purposes).
- f. Incorporates information to meet the requirements of the COPPA, where appropriate (see section 4.4).
- g. Notifies visitors as to how the Agency handles unsolicited e-mail, including the fact that the sender's privacy is not guaranteed.

4.3.2 Web site curators shall clearly post a link to the NASA Web Privacy Policy on the home page of all NASA Web sites, modified as necessary to accurately reflect their specific Web sites (e.g., to indicate the collection of persistent cookies (see section 4.4.6.c)).

4.3.3 Web site curators shall ensure that links to the NASA Web Privacy Policy are:

- a. Clearly labeled "Privacy Policy and Important Notices."

b. Easily accessible by all visitors to a Web site.

4.3.4 Web site curators shall ensure that machine readable technology is used that alerts users automatically about whether site privacy practices match their personal privacy preferences.

4.3.5 Posting of the NASA Web Privacy Policy is not required if:

a. A Web site is comprised solely of information other than "Government information" as defined in OMB Circular A-130 (i.e., information created, collected, processed, disseminated, or disposed of by or for the Federal Government).

b. A Web site is an Agency intranet Web site accessible only by authorized NASA users (employees, contractors, consultants, fellows, and grantees).

c. A Web site is for a national security system defined in 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Gov Act).

4.4 Collecting PII

4.4.1 If Web sites collect PII, Web site curators shall ensure that their privacy policies clearly and concisely inform visitors to the site about the following:

a. Any PII collected or proposed to be collected.

b. Why the information is collected.

c. How the information is collected (if not apparent).

d. How the visitor can avoid or disable the collection mechanism if so desired.

e. How the information that is collected will be used, including retention and disposition information.

f. Whom to contact to access the information collected about them.

4.4.2 If a NASA Web site collects PII that qualifies as a Privacy Act SOR, the RNO for the site shall ensure that all Privacy Act requirements are met.

4.4.3 RNOs shall maintain the confidentiality, security, and integrity of any PII their Web sites collect.

4.4.4 NASA Web sites that are intended for use by children and that collect PII from children who are under the age of 13 are subject to the requirements of COPPA. See Appendix G for additional information to assist in determining the applicability of COPPA. For Web sites subject to COPPA, Web site curators shall:

a. Eliminate the collection of information if the information is not essential to a NASA program.

b. Incorporate notice of the information collection practices into the Web Privacy Policy for their site, providing users with the following information:

(1) A description of what specific types of PII are collected from children (e.g., name, age, home address, e-mail address, or hobbies) and whether any additional information is collected passively (e.g., through cookies).

(2) A description of how the information will be used (e.g., to make the information available through a child's participation in a chat room) and whether PII is shared with third parties.

(3) How long the information will be maintained.

(4) Who will have access to the information.

(5) A contact name and information (address, telephone, e-mail address) for the site.

c. Web site RNOs shall make reasonable efforts to ensure that parents or legal guardians of children receive notice of the site's information collection practices and obtain verifiable parental consent to those practices before PII is collected from a child. Further elaboration on the parental notice is contained in Appendix G.

(1) Upon request from the parent or legal guardian, the RNO shall provide a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child.

(2) RNOs shall ensure that parents are provided with the right to revoke their consent and ask that information about their children be deleted from the site database at any time.

(3) When a parent revokes consent, the Web site RNO shall ensure that collection, use, or disclosure of information from that child is ceased immediately.

d. The Web site RNO shall also obtain parental consent when the site:

(1) Considers a change to the kinds of information previously collected.

(2) Changes how the information is used.

(3) Offers the information to new or different third parties.

(4) Uses the information in a way that is different than how it was specified when parental consent was originally obtained.

(5) Gives a child access to a secondary site that was not originally specified in the Web site notification.

e. Instances when parental consent is not necessary are discussed in Appendix G.

f. The Web site RNO shall ensure that PII is disclosed only to individuals internal to NASA who have a business requirement for the information or to those individuals external to the Agency in accordance with "routine uses" published in a Privacy Act SORN.

g. The Web site curator shall ensure that an exit notice is placed between the COPPA site and any external links stating that NASA is not responsible for the material found on, or the data collection activities of, the external Web pages. This provides clear notification to both the child and the parent that they are exiting the NASA domain and that NASA can no longer guarantee the security of their information.

h. RNOs shall not condition a child's participation in a game, the offering of a prize, or another activity on the child's disclosing of more personal information than is reasonably necessary to participate in such activity.

4.4.5 NASA Web site RNOs shall ensure that Web sites do not use persistent cookies on public NASA Web sites unless all of the following conditions are met:

a. The RNO determines that there is a compelling need to collect the data on the site (e.g., site enhancement, navigational assistance for returning visitors, or similar needs).

- b. The Web site RNO has received prior approval from the NASA CIO to use persistent cookies.
- c. The Web site provides clear and conspicuous notice concerning its use of cookies or other automatic means of collecting information.
- d. The Web site includes appropriate and publicly disclosed privacy safeguards for how information derived from "cookies" will be handled and maintained.

4.4.6 When a public Web site uses persistent cookies:

- a. The RNO shall prepare a memorandum requesting a waiver to use persistent cookies to be addressed to the NASA CIO through the NASA Associate Chief Technology Officer (CTO) and the NASA Privacy Act Officer. A waiver template is provided in Appendix C.
- b. The RNO shall annually seek a continuation of a previous NASA OCIO waiver for the use of persistent cookie technology as long as the use requirement remains.
- c. The site curator shall post, as part of the site's Privacy Policy, clear and conspicuous notices about the site's use of cookies or other automatic means of collecting information. The notice must include:
 - (1) The nature of the information collected.
 - (2) The purpose and use of the information.
 - (3) Whether, and to whom, the information will be disclosed.
 - (4) The privacy safeguards applied to the information collected.
 - (5) The consequences of opting out (e.g., the application the visitor wishes to use may not work correctly without the cookie).
- d. Further information describing cookies, the preparation of waiver requests, and the required notice are contained in Appendix G.

Chapter 5. Privacy Act Systems of Records

5.1 General

This chapter, together with 14 CFR 1212, provides specific requirements for the management of Privacy Act SORs throughout their life cycles. Further guidance for implementing these requirements may be found in Appendix H. Because the Privacy Act specifically refers to PII contained in SORs as Privacy Act "records," this chapter uses the term "records" as defined by the Privacy Act.

5.2 Creating or Modifying a Privacy Act SOR

5.2.1 The Center PAM shall manage the process for creating, amending, or deleting an authorized SOR at his/her Center. The PAM should ensure that no appropriate existing NASA or Government-wide SOR exists prior to initiating a new SORN.

5.2.2 When developing or modifying a Privacy Act SOR and prior to any collection or new use of information in such a system, the system owner (called "system manager" in this chapter in accordance with the Privacy Act and 14 CFR 1212) shall, in coordination with his/her Center PAM, draft a SORN for publication in the Federal Register and provide it to the Privacy Act Officer. While details on this process may be found in Appendix H and an annotated SOR template is available on the NASA OCIO Privacy Web site, the basic required elements of a SORN include:

- a. The name and location of the system.
- b. The categories of individuals on whom records are maintained in the system.
- c. The categories of records maintained in the system.
- d. The authority for maintenance of the system.
- e. Each routine use of records contained in the system, including the categories of users and the purpose of such use.
- f. Policies and practices regarding the storage, retrievability, access controls, and retention and disposal of the records.
- g. System manager(s) and address(es).
- h. Agency procedures whereby an individual may request information as to whether the system records pertain to him/her.
- i. 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.
- j. The categories of sources of records in the system.

5.2.3 The Privacy Act Officer shall review the draft notice and coordinate the Headquarters review and the NASA CIO's signature for submittal to the Federal Register for publication through the NASA Federal Register Liaison Officer.

5.3 Collecting Information for a Privacy Act SOR

5.3.1 The system manager shall ensure that information on individuals that is collected and maintained in a SOR is done so in accordance with 14 CFR 1212. Particular care should be taken to avoid the collection of social security numbers (SSNs), in accordance with NPD 1382.17G, unless required by statute or some other requirement mandating the use of SSNs.

5.3.2 System managers shall ensure that individuals who are asked to provide information to be maintained in a Privacy Act SOR are first presented with a Privacy Act Statement, either on the information collection sheet or screen or via a separate sheet or screen that the individuals can print and retain. Such a statement must comply with the requirements outlined in 14 CFR 1212.602, and individuals must be able to retain a hard copy of the Privacy Act Statement. Appendix H provides guidance on possible methods of providing a Privacy Act Statement under different collection circumstances.

5.3.3 System managers shall ensure that new NASA forms or Center forms created for the collection of SOR information also provide the Privacy Act statement for that SOR.

5.4 Using Privacy Act Records

5.4.1 For electronic systems containing records with Privacy Act information, system managers shall ensure that a system notification is provided to anyone entering the system. The notice must explain that records in the system are subject to the Privacy Act and that it is illegal to willfully disclose information to individuals not entitled to it. A sample of this notice is contained in figure 5.1.

5.4.2 Employees shall limit disclosure of information concerning individuals from a SOR in accordance with 14 CFR 1212 or with routine uses of the records as published in the SORN. Employees may be subject to criminal penalties for willful and intentional violations of the Privacy Act.

5.4.3 System managers shall control disclosures from their SOR and maintain accountings of all disclosures of information in accordance with 14 CFR 1212.203.



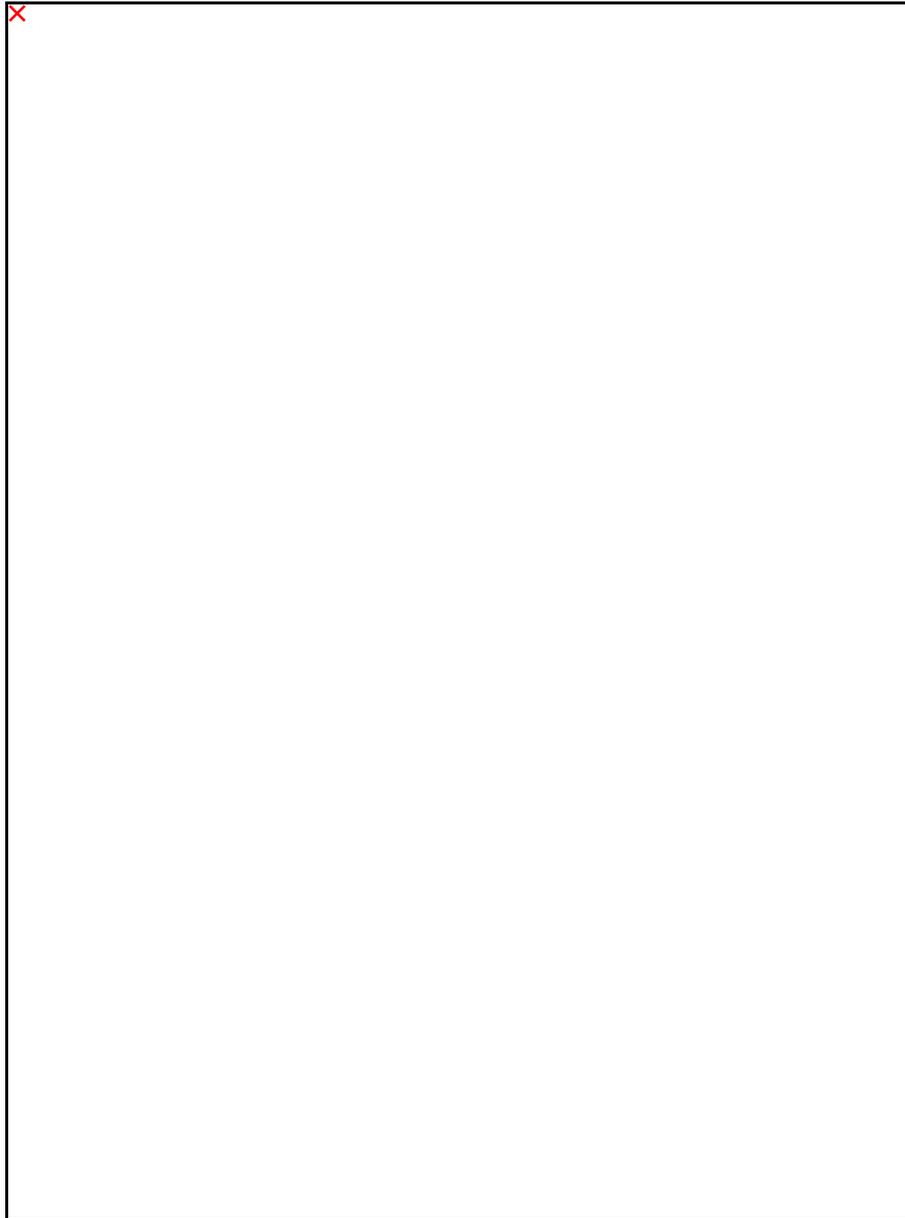


Figure 5.1 Privacy Act Statement

5.4.4 When transmitting material subject to the Privacy Act, employees shall perform the following actions:

- a. In hard copy format, include a watermark "NASA Privacy Information, Protect Accordingly" on each individual page and cover the material with NASA Form (NF) 1532, Privacy Act Cover Sheet.
- b. In electronic format, encrypt in accordance with NPR 1600.1.

5.4.5 The NASA CIO shall establish a Data Integrity Board in accordance with the Privacy Act before any system manager may engage in a computer matching program as defined by the Privacy Act. The Data Integrity Board will approve, oversee, and coordinate the matching program.

5.4.6 Prior to the establishment or revision of a matching program, the system manager of the SOR involved shall prepare a SORN, to be coordinated by the Privacy Act Officer, for publication in the Federal Register at least 30 days in advance in accordance with the PA.

5.5 Maintaining and Disposing of Privacy Act Records

5.5.1 System managers shall ensure that records are maintained in accordance with 14 CFR 1212.

5.5.2 System managers shall ensure the development and documentation of administrative, technical, and physical safeguards that protect against any anticipated threats or hazards to the security or integrity of records and against their unauthorized use.

5.5.3 The system manager shall ensure that persons involved in the design, development, operation, or maintenance of any SOR, or in the maintenance of any record in any SOR, are trained in the requirements regarding the protection, use, and release of such records.

5.5.4 System managers shall ensure the implementation of procedures to dispose of system records only in accordance with applicable approved retention schedules contained in the NASA Records Retention Schedules (NRRS) and the NPR 1600.1 procedures for disposing of SBU information.

When NASA provides by contract for the operation of an SOR on behalf of the Agency, the contractor is subject to all requirements of the Privacy Act and this chapter. The system manager shall ensure that the contract:

- a. States that the Privacy Act applies.
- b. Includes appropriate FAR citations from FAR 52.224.

Appendix A. Glossary

Term	Definition
Application (defined in NPR 2810.1A)	The use of information resources (information and information technology) to satisfy a specific set of user requirements (reference OMB A-130). Also, a set of computer commands, instructions, and procedures used to cause a computer to process a specific set of information. Application software does not include operating systems, generic utilities, or similar software that is normally referred to as "system software."
Application Owner	An agency official with statutory or operational authority for specified applications and with the responsibility for requirements analysis, design, development, and sustaining engineering of the specified application. The application owner may or may not be the same as the Information Owner.
Contract (defined in Federal Acquisitions Regulations 2.102)	A mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications.
Computer Matching Program (defined in the Privacy Act)	<p>Any computerized comparison of:</p> <p>(1) two or more automated systems of records or an SOR with non-Federal records for the purpose of: (a) establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs; or (b) recouping payments or delinquent debts under Federal benefit programs.</p> <p>(2) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records.</p>

Cookies	A cookie is a small file that a Web site transfers to a user's computer to allow the computer to remember specific information about the user's session while connected. The user's computer will share the information in the cookie only with the Web site that provided it, and no other Web site can request it. There are two types of cookies: session and persistent. Session cookies last only as long as the user's Web browser is open. Once the browser is closed, the cookie disappears. Persistent cookies store information on a user's computer for longer periods of time.
Database	A comprehensive collection of related data organized for convenient access, generally in a computer.
Exit Page	An intermediary page the user sees before proceeding to external Web pages not located on NASA servers; it notifies users that they are leaving NASA-managed Web pages.
Individual (defined in the Privacy Act)	A citizen of the United States or an alien lawfully admitted for permanent residence.
Information Collection (defined in 5 C.F.R. 1320.3(c)(1))	Information collection can occur in any form or format, including the use of report forms; application forms; schedules; questionnaires; surveys; reporting or recordkeeping requirements; contracts; agreements; policy statements; plans; rules or regulations; planning requirements; circulars; directives; instructions; bulletins; requests for proposals or other procurement requirements; interview guides; oral communications; posting, notification, labeling, or similar disclosure requirements; telegraphic or telephonic requests; automated, electronic, mechanical, or other technological collection techniques; standard questionnaires used to monitor compliance with agency requirements; or any other techniques or technological methods used to monitor compliance with agency requirements.
Information in Identifiable Form (defined in OMB Memorandum M-03-22)	Information in an IT system or online collection: (a) that directly identifies an individual (e.g., name, address, SSN, or other identifying number or code, telephone number, e-mail address, etc.) or (b) by which NASA 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.)

Information Owner (defined in NPR 2810.1A)	An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information System (defined in OMB Circular A-130)	The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.
Information Technology (defined in NPR 2810.1A)	Any equipment, software, or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
Information Technology (IT) System	See Information System.
Internet Protocol Security	A suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream.
Kids' Pages	NASA Web sites directed to children who are under 13 years of age.
Major Information System (defined in OMB Circular A-130)	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Member of the Public	Under the E-Gov Act, members of the public are individuals other than government personnel, government contractors, and government consultants and partners. However, under the PRA, government contractors and government consultants and partners may be considered to be members of the public.
NASA Cognizant Official	NASA civil servant responsible for management of daily operations of an IT system.

National Security System	Information system operated by NASA, the function, operation, or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons system, or (e) systems critical to the direct fulfillment of military or intelligence missions. This does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management.
Personally Identifiable Information (defined in OMB Memorandum M-06-19)	<p>Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.</p> <p>For purposes of NASA policy, PII excludes personal information collected and or maintained by NASA employees and contractors for personal rather than NASA business purposes as allowed under NPD 2540.1 Personal Use of Government Office Equipment Including Information Technology. Examples of such excluded data include contact information for family, relatives, and doctors.</p>
Personal Identifier	A name or the identifying number, symbol, or other unique identifier such as the SSN or user ID number assigned to an individual.
Privacy Impact Assessment (defined in OMB M-03-2s)	An analysis of how information is handled/controlled to: (a) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (b) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (c) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privacy Act	Privacy Act of 1974, as amended (5 U.S.C. 552a).
Privacy Policy in Standardized Machine-Readable (also known as "P3P") Format	A statement about site privacy practices written in eXtensible Markup Language (XML) that can be read automatic-ally by a Web browser.

<p>Record (as specifically defined by the Privacy Act)</p>	<p>Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to: that individual's education, financial transactions, medical history, and criminal or employment history and that contains an individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voice print or a photograph.</p> <p>This definition is not the same as "record" as defined by the Federal Records Act.</p>
<p>Responsible NASA Official (RNO)</p>	<p>A NASA civil service employee responsible for a NASA Web page or Web application. The RNO is accountable for reviewing and approving the accuracy, timeliness, and appropriateness of information posted on a Web site, making sure that both the content and structure comply with applicable policies and guidelines.</p>
<p>Routine Use (defined in the Privacy Act)</p>	<p>With respect to the disclosure of a record, the use of a record for a purpose compatible with the purpose for which it was collected.</p>
<p>Secure Socket Layer</p>	<p>A cryptographic protocol which provides secure communications on the Internet.</p>
<p>System Manager (defined in 14 CFR 1212)</p>	<p>The NASA official who is responsible for a system of records as designated in the system notice of that system of records published in the Federal Register. When a system of records includes portions located at more than one NASA installation, the term system manager includes any subsystem manager designated in the system notice as being responsible for that portion of the system of records located at the respective Installation.</p>
<p>System of Records (defined in the Privacy Act)</p>	<p>A group of any records under NASA's control that contains information about individuals from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier particular assigned to the individual.</p>
<p>System Owner</p>	<p>The individual responsible for establishing the rules for appropriate use and protection of the data/information within a system. The system owner retains that responsibility even when the data/information are shared with other organizations.</p>

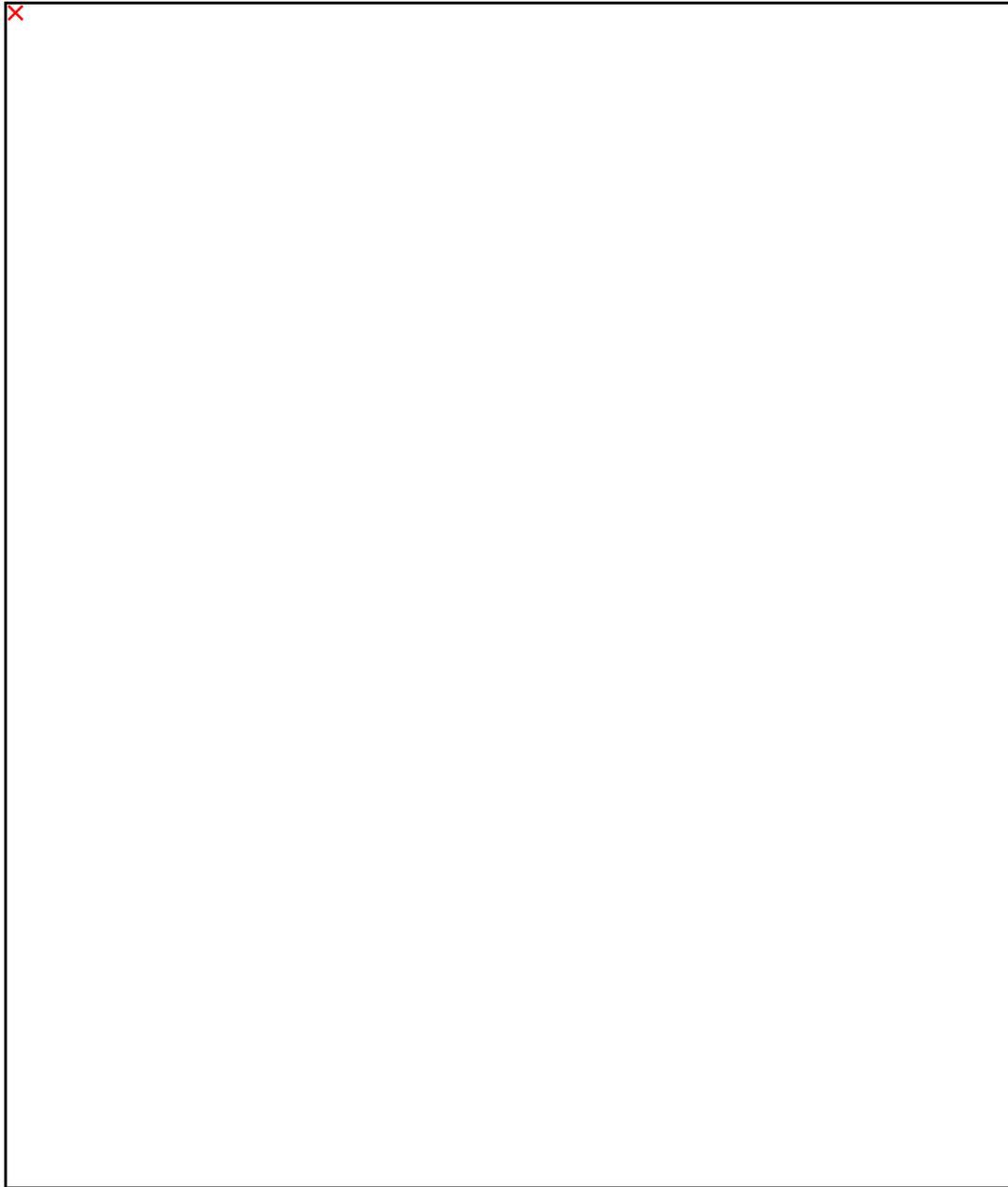
Verifiable Parental Consent (from Children's Online Privacy Protection Act of 1998)	Any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.
Virtual Private Network	A private communications network often used by companies or organizations to communicate confidentially over a public network.
Web Site Curator	Individual who maintains a Web site, for example, updating text, pictures, and links.
Web Site Developer	Individual who creates Web sites and Web applications, including designing layout, programming, writing text, creating graphics, and adding pictures and links.

Appendix B. Acronym List

C&A	Certification and Accreditation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COPPA	Children's Online Privacy Protection Act of 1998
CTO	Chief Technology Officer
EA	Enterprise Architecture
E-Gov Act	E-Government Act of 2002
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GPRA	Government Performance and Results Act of 1993
GRS	General Records Schedule
IC	Information Collection
ICR	Information Collection Request
IIF	Information in Identifiable Form
IP	Internet Protocol
IPSec	Internet Protocol Security
IPTA	Information and Privacy Threshold Analysis
IT	Information Technology
JPL	Jet Propulsion Laboratory
NF	NASA Form
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NRRS	NASA Records Retention Schedule
OCIO	Office of the (NASA) Chief Information Officer
OMB	Office of Management and Budget
P3P	Privacy Policy in Standardized Machine-Readable
PAM	Privacy Act Manager
PDF	Portable Document Format
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PRA	Paperwork Reduction Act
RNO	Responsible NASA Official
SBU	Sensitive But Unclassified
SOR	System of Records
SORN	System of Records Notice

SSL	Secure Socket Layer
SSN	Social Security Number
URL	Uniform Resource Locator
XML	eXtensible Markup Language

Appendix C. Tracking Waiver Template



Appendix D. References

- a. OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources.
- b. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Gov Act.
- c. OMB Memorandum M-06-16, Protection of Sensitive Agency Information.
- d. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments.
- e. NASA ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting.
- f. Memorandum from the NASA Chief Information Officer regarding NASA Web Site Linking Policy, NASA Internal Memorandum, dated December 19, 2005.

Appendix E. Privacy Actions by Information Stage

All PII, regardless of form, must be protected from unauthorized access or unauthorized disclosure throughout its life cycle as SBU information in accordance with NPR 1600.1. Required actions must be taken for information systems containing PII and the management of PII at different phases in the life cycle of information systems and the information itself.

E.1 Systems Planning/Development

The type of information to be collected/maintained and how it is managed dictate the requirements for information systems and Web sites in planning and development that must be met prior to system implementation.

- a. If an information system will collect/maintain PII, it or the system that hosts such an application must be assigned a FIPS 199 security categorization of at least Moderate, and corresponding security controls implemented.
- b. If information is collected from the public through the use of standard fields, whether voluntarily or not and regardless of collection media, the collection process must be assessed further by the NASA PRA Officer in the NASA OCIO for PRA applicability. If an OMB authorization as a PRA information collection (IC) is required, steps must be taken to obtain OMB authorization.
- c. If the system will constitute a Privacy Act SOR, a SORN describing the system must be published in the Federal Register.
- d. If any information is to be collected through a Web site using persistent cookies, there must be a compelling need to do so and a waiver for persistent cookie use obtained from the NASA CIO.
- e. System/Web site content must be evaluated using the IPTA available through the NASA OCIO Web site.
- f. If IIF on members of the public is to be collected/maintained, or if any IIF is to be collected/maintained and the system requires an EA review, the full PIA will be conducted.

E.2 Collection Requirements

NASA may only collect/maintain information about individuals that is relevant and necessary to accomplish a purpose of the Agency required by statute or Executive Order of the President.

E.2.1 Collection methods used by NASA systems or applications to obtain information, whether electronically or otherwise, include forms (electronic and hard copy), interviews or telephone conversations, surveys/questionnaires, inputs from other Government systems or other sources, persistent tracking technology on Web sites, Web-enabled forms, or e-mail links.

E.2.2 NASA collects and/or maintains information on civil servants, contractors and partners, and members of the public, including children or employee families. In all cases, at the point of collection of information on individuals, notification of the purpose and intended use of the information must be presented to the person providing the information. Specifics regarding the notification, elaborated in Chapters 4 and 5, vary slightly depending on which statutes apply as

indicated below:

- a. If any PII is collected via a Web site from members of the public, whether through persistent cookies or not, notification requirements of the E-Gov Act apply.
- b. If Web sites target and collect PII from children under age 13, COPPA notices and processes are required.
- c. Regardless of how or on whom information about individuals is collected/maintained, if maintained data are or will be retrieved by name or other unique personal identifier, Privacy Act notification requirements apply.

E.3 Maintenance Requirements

- a. Owners of systems collecting/maintaining PII must ensure the maintenance of current, accurate, relevant, and complete information and its protection against unauthorized alteration, access, use, or disclosure.
- b. Protection of information must be assured through risk management, system security procedures, including maintenance of system security controls corresponding to their assigned security categories, and IT Security C&A in accordance with NPR 2810.1.
- c. Employees must report any suspected or confirmed IT security incident involving PII, whether in physical (non-electronic) or electronic form, immediately upon discovery in accordance with NPR 2810.1.

E.4 Utilization Requirements

E.4.1 Owners of systems that are collecting and/or maintaining PII must describe, through the following mechanisms as appropriate, the ways in which the information is used by the Agency:

- a. SOR Notices published in the Federal Register.
- b. PIAs.
- c. PRA IC authorization requests.
- d. Notifications to individuals on whom information is being collected/maintained.
- e. Web site policy statements.

E.4.2 Owners of systems containing PII must ensure that access is limited to those Agency employees who have a need for the information in the performance of their duties or, in the case of Privacy Act records, to disclosures outside the Agency (even to contractors) pursuant to a routine use published in the Federal Register.

E.4.3 Users with access to information in NASA Privacy Act SORs must be:

- a. Notified at each entry into a system (when electronic) that it contains PII that must be protected and not disseminated without authorization.
- b. Trained as to their responsibilities regarding access to, as well as use and protection of, the PII.

E.5 Dissemination Requirements

E.5.1 Data dissemination, sharing, or any sort of disclosure of IIF inside or outside the Agency must be limited to:

- a. The purposes for which the information was collected.
- b. Routine uses described in Privacy Act SORs.
- c. NASA employees who require the information to accomplish their jobs.
- d. Compliance with the written request or consent of the individual on whom the data are maintained.

E.5.2 Individuals' names and addresses may not be sold or rented unless such action is specifically authorized by law.

E.5.3 When transmitting privacy data via e-mail messages, senders must encrypt the messages prior to transmission, in accordance with NPR 1600.1.

E.5.4 When transmitting, in hard copy format, privacy data that are subject to the Privacy Act, the material should be covered with NF 1534, "Privacy Act Cover Sheet." When transmitting any other hard copy privacy data, they should be covered with NF 1686, "Sensitive But Unclassified (SBU)." Both should be handled as SBU information in accordance with NPR 1600.1. Any hard copy material containing PII must include a watermark, "NASA Privacy Information, Protect Accordingly," on each individual page.

E.6 Disposition Requirements

When system information qualifies as Federal records as defined in the NRRS, system owners must ensure that records are managed and disposed of in accordance with the NRRS or GRS.

Appendix F. Guidance for Privacy Impact Assessments

F.1 System Changes Requiring PIAs

As discussed in Chapter 3, changes to systems that may create new privacy risks and thus require a new PIA include, but are not limited to:

- a. Conversions of paper-based records to electronic systems.
- b. The application of functions to an existing information collection that change anonymous information into non-anonymous IIF.
- c. New uses of an existing IT system, including the application of new technologies that significantly change how IIF is managed in the system.
- d. Adoption or alteration of business processes so that databases holding IIF are merged, centralized, matched with other databases, or otherwise significantly manipulated.
- e. New application of user-authenticating technology (e.g., password, digital certificate, biometric elements) to an electronic information system that is accessed by members of the public.
- f. Systematic incorporation into existing information systems databases of IIF that are purchased or obtained from commercial or public sources. However, mere querying of such a source on an ad hoc basis using existing technology does not trigger the PIA requirement.
- g. NASA cooperation with another agency or agencies on shared functions involving significant new uses or exchanges of IIF, such as crosscutting E Government initiatives. In such cases, the lead agency has the responsibility for preparing the PIA.
- h. Alteration of a business process that results in significant new uses, disclosures of information, or incorporation into the system of additional items of IIF.
- i. Addition of new IIF to a collection resulting in increased risks to personal property (e.g., addition of health or financial information).

F.2 Circumstances of Unchanged Privacy Issues Requiring No PIA

As discussed in Chapter 3, examples of circumstances of unchanged privacy issues for systems or Web sites such that a PIA is not required include, but are not limited to:

- a. Government-run Web sites, IT systems, or collections of information to the extent that these do not collect or maintain IIF concerning members of the public, excluding NASA contractors and partners.
- b. Government-run public Web sites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or obtaining additional information.
- c. National security systems that are defined by 40 U.S.C. 11103 as exempt from the definition of

information technology.

d. Minor changes to a system or collection that do not create new privacy risks.

F.3 How to Conduct a PIA

F.3.1 If a PIA is required, as evidenced by a completed IPTA, the system owner must access and complete the PIA Worksheet via the NASA OCIO Web site.

F.3.2 Specific features of the information system will be reviewed and documented during the conduct of a PIA.

F.3.3 In completing the PIA, a number of factors concerning the content, nature, and use of information that is to be collected must be described, including:

- a. Explanation of how and why that information is being collected (e.g., to determine eligibility).
- b. The intended use of the information (e.g., to verify existing data).
- c. Specifics concerning with whom the information will be shared (e.g., another agency for a specified programmatic purpose).
- d. The opportunities individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), together with information on how individuals can grant consent.
- e. Whether it contains Federal records or organizational vital records.
- f. Whether the records contained by the system are covered under an approved disposition schedule.
- g. Whether a SOR is being created for the system under the Privacy Act, 5 U.S.C. 552a.

F.3.4 A description must be provided as to how the information will be secured via administrative and technological controls.

F.3.5 The PIA summary must include not only a summary of the completed worksheet, but also any decisions NASA made regarding the IT system or application as a result of performing the PIA.

F.4 Coordinating Completion of a PIA with PRA Requirements

F.4.1 When undertaking new electronic information collections as defined under the PRA, the system owner may submit the PIA and make it publicly available as part of the Supporting Statement of the request to OMB for approval of a new agency information collection. System owners must work through the PRA Officer in the NASA OCIO to request OMB approval to collect information under the PRA.

F.4.2 If submitting a Joint Information Collection Request (ICR) and PIA, all elements of the PIA must be addressed by the system owner and identifiable within the structure of the ICR Supporting Statement to the ICR, including:

- a. A description of the information to be collected.
- b. An explanation of how the information will be shared and for what purpose.
- c. An account of the impact the proposed collection will have on privacy.

d. A description of how the information will be secured and whether a SOR is being created under the Privacy Act.

F.4.3 The PRA Officer in the NASA OCIO should be consulted for additional information on the PRA requirements and compliance criteria.

F.4.4 System owners are not required to conduct a new PIA when simply processing PRA information collection renewal requests. Rather, in accordance with section 3.2 of this document, the need for a PIA must be separately considered when amending an ICR to collect information that significantly differs in character from the original collection.

F.5 Coordinating PIA Completion with Preparing a SORN

If the information in the system constitutes a Privacy Act SOR for which a new SORN is required, systems owners:

- a. May conduct a PIA concurrently with the SOR Notice required by the Privacy Act, if required, since the PIA and the SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).
- b. May request that the Privacy Act Officer make the PIA publicly available in the Federal Register along with the Privacy Act SOR notice.

Appendix G. Web Privacy Guidance

Information in this appendix does not duplicate, but expands on, the Web site requirements contained in Chapter 4.

G.1 Privacy Act Web Sites

G.1.1 If a NASA Web site collects PII that will be maintained and will, in practice, be retrieved by name or personal identifier, that information is protected under the Privacy Act, and the NASA RNO must ensure that a valid Privacy Act SORN is published in the Federal Register prior to data collection (see Chapter 5 of this NPR).

- a. Prior to drafting a new Privacy Act SORN, the RNO of the Web site collecting Privacy Act information should coordinate with his or her Center PAM to determine whether an existing SORN adequately provides for the maintenance of the information (records) to be collected.
- b. For such a Web site, the RNO must ensure that a Privacy Act Statement is presented at the point of information collection. See Chapter 5 and Appendix H for Privacy Act compliance procedures.
- c. Information collected using cookies (see Chapter 4) and Web server logs is not covered by the Privacy Act unless the information collected is routinely retrieved by a personal identifier.

G.2 COPPA Web sites

G.2.1 Determining COPPA applicability. Factors to be considered in determining whether a Web site is directed to children under 13 years of age include the subject matter, visual or audio content, the age of models on the site, language, whether advertising on the Web site is directed at children, information regarding the age of the actual or intended audience, and whether a site uses animated characters or other child-oriented features.

G.2.2 Exceptions to required parental consent. Parental consent is not necessary if the Web site collects a child's PII to:

- a. Respond to a one-time request from the child (e.g., providing a poster, responding to a question, etc.) after which the IIF is deleted.
- b. Contact the parent.
- c. Ensure the safety of the child or the site.
- d. Fulfill a NASA newsletter request for a single issue (continuation of a subscription requires consent).

G.3 PRA Web sites

Web sites that collect or sponsor the collection of information from ten or more respondents through identical fields (e.g., via online forms, surveys, or printable PDF (portable document format) forms) may be subject to the PRA, regardless of whether information is in identifiable form. The need or plan to collect any such information from the public must be cleared with the PRA Officer in the NASA OCIO as to PRA applicability.

G.4 Web Sites Using Persistent Cookies

G.4.1 To obtain approval for the use of persistent cookies on a public Web site, the Web RNO shall submit a written request to the NASA Privacy Act Officer who will review and forward it, along with a recommendation, to the NASA CIO for approval.

G.4.2 Waiver request.

a. The waiver request must include:

- (1) Identification of the Web site for which the waiver is sought.
- (2) A complete description of all information the cookie will collect.
- (3) A detailed description and justification of the purpose of the cookie.
- (4) How long the cookie will stay on the user's computer.
- (5) How the information collected will be maintained and who will have access to it (e.g., whether it will be shared with third parties).
- (6) The proposed notice that will be displayed on the Web site using the cookie (upon approval) that clearly states to the user of the site information reported in section 4.3.5.c below.
- (7) The name of the contact person for cookie information.

b. As long as the use requirement remains, renewal of the waiver must be requested annually. The waiver renewal request must verify the continued compelling need to use persistent cookies and include the original and previous years' waivers as attachments.

G.4.3 Persistent cookie explanation in Privacy Web policy. For the convenience of curators, the cookie section of the NASA Web Privacy Policy contains a placeholder for adding the notice. A good practice is to provide additional notice on or before the page where the cookie is set (the point of collection).

Appendix H. Privacy Act Guidance

Information in this appendix does not duplicate, but expands on, SOR requirements contained in Chapter 5.

H.1 Systems that Do Not Qualify as SORs

Systems that only collect NASA employees' or contractors' names and work-related information (such as work e-mail address, office location, and office telephone number) do not qualify as Privacy Act SORs, although the data may be retrieved by individuals' names, because the PII is not personal information to be protected.

H.2 Developing a SORN

H.2.1 The system manager, with the assistance of the Center PAM, will draft a Federal Register notice of the system for the NASA CIO's signature. The Center PAM will coordinate Center legal review for Center-specific systems and submit the notice to the Privacy Act Officer for Agency-level review. An annotated SORN format may be found on the NASA Privacy Web site.

H.2.2 SORN Content. The first few fields of the SORN, through "Supplementary Information," constitute the notice preamble and must be prepared in accordance with the Federal Register Document Drafting Handbook, 1998 edition. The remaining fields specifically describe the SOR and must include:

- a. The name and location of the system. The name describes the records maintained in the system or the individuals on whom the records are maintained. The system location specifically identifies each address or location at which records are physically maintained; for a system with many locations, the list of addresses and locations may be included by reference to the NASA System of Record Notice, Appendix B, as published with existing NASA SORNs.
- b. The categories of individuals on whom records are maintained in the system. Categories of individuals covered by the system must be identified. The identification must be specific, and it must be stated in a manner that is clearly understood by the general public. Existing system notices may serve as examples of how to describe categories of individuals.
- c. The categories of records maintained in the system. Each type of record or information maintained in the system must be identified as specifically as possible. This must be an all-inclusive list, and the record description must be clear and understandable to the general public. Acronyms, abbreviations, and references to public laws and regulations are to be avoided. For records containing many data fields, efforts must be made to list larger groupings that comprehensively incorporate the nature of all of the smaller detailed fields maintained. For example, "U.S. visitor/travel document numbers" may cover both passport and visa numbers, while "employment information" may cover employers' names and addresses.
- d. The authority for maintenance of the system. The specific statutory provision(s) that authorize(s) the solicitation and maintenance of the information in the SOR must be identified. The authority must be statutory, not regulatory; that is, it must cite the United States Code or public law rather than the Code of Federal Regulations or Agency policies.
- e. Each routine use of records contained in the system, including the categories of users and the

purpose of such use. These are brief, concise, and clear statements of the disclosures of the information that may be made from the SOR. The term "routine use" strictly means the disclosure of a record or information from the system to entities outside the Agency for a purpose 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 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 such disclosure is requested by a third party.) The statement must specify, by reference to the numbers from NASA SORN, Appendix B, any "standard routine uses" that apply to the system and attach it to this document.

f. Policies and practices regarding the storage, retrievability, access controls, and retention and disposal of the records. Each of these items must be discussed separately, each with its own paragraph heading.

(1) For policies and practices regarding storage, the medium and/or manner in which the records are maintained should be described, e.g., on microfilm, on magnetic tape, on a server, on a CD, or in paper file folders. If this varies by location, such as at different Field Centers, the storage at each location should be explained.

(2) For policies and practices regarding retrievability, the data fields by which records are indexed and routinely retrieved should be explained.

(3) For policies and practices on access controls, measures taken to prevent unauthorized access and disclosure of records, e.g., physical security, personnel screening, or technical safeguards, should be briefly described. Safeguards from natural disasters (e.g., tornadoes) should be included, along with backup and offsite storage and operations to be used 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 insufficient. Citing existence of an approved IT Security Plan or mentioning that "analyses of the system were conducted as required by FIPS 199 and applicable security con-trols implemented in accordance with FIPS 853" may serve as additional evidence that proper security measures were evaluated and implemented for electronic systems.

(4) For policies and practices regarding the retention and disposal of records, the approved disposition authority under which the records are retained and archived or disposed of should 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)." The NASA Privacy Act Officer will not concur with the SORN for publication unless either an approved retention schedule is cited or a draft new schedule item is submitted with the SORN. System managers should coordinate with their Center Records Manager to identify a proper retention schedule item or to develop a schedule item for submission to the NASA Records Officer. The records may not be destroyed until NASA obtains an approved records disposition schedule from the Archivist of the United States.

g. System Manager(s). The title, office symbol, and address of the Agency official responsible for the policies and practices governing the SOR must be provided. Individual names are not included to ensure that the SORN does not become outdated due to NASA personnel changes. If the system of records is maintained in physically separate locations, other managers are to be listed as subsystem managers by their Center position titles and their addresses provided. Locations and addresses may be listed by reference to SORN Appendix B, which is the appendix for NASA's comprehensive SOR Notices as published in the Federal Register.

h. Agency procedures whereby an individual may request information as to whether the system contains records pertaining to them. The address(es) must be provided for the NASA office(s) to which inquiries are to be sent and the address(es) of the location(s) at which the individual may present a request as to whether a system contains records pertaining to him/her. Include any identifying information an individual is required to provide so that the Agency may determine whether the system contains a record about that individual.

i. Agency procedures whereby an individual can request access to any record contained in the SOR that pertains to him/her and learn how he or she can contest its content. The name(s) and address(es) must be provided for the NASA office(s) to which the individual may write to obtain information from his/her record. This information is for the individual who already knows that a system contains information about him/her.

j. The categories of sources of records in the system. The source of the records or information in the system (e.g., whether the information comes directly from individuals themselves, from other SORs, or from some other entity or Government unit) must be described as specifically as possible.

H.2.3 Once concurrence has been received from the PAM and the Office of the Chief Counsel, the local PAM will submit the notice to the Privacy Act Officer for processing.

H.2.4 The Privacy Act Officer will review the draft notice and coordinate review by the Office of the General Counsel and the NASA CIO for signature. 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.

H.3 Privacy Act Statement

As discussed in Chapter 5, system managers must ensure that individuals are presented with a Privacy Act Statement meeting the requirements outlined in 14 CFR 1212.602. Table H.1 addresses how to provide a Privacy Act statement under different collection circumstances.

Table H.1 Privacy Act Statement Delivery Requirements

Collection Method	Examples	NASA Procedures to Provide a Privacy Notice
In person	• Interviews	<ul style="list-style-type: none"> • Content of the notice must meet the requirements specified in this chapter. • 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	<ul style="list-style-type: none"> • Clinic forms • Printed forms requiring signatures 	<ul style="list-style-type: none"> * Content of the notice must meet the requirements specified in this chapter. * Place the notice on the form near where data are collected or provide a separate Privacy Act Statement before collecting the data.
Telephone	<ul style="list-style-type: none"> * Information collected for NASA visitor clearance 	<ul style="list-style-type: none"> • 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 the caller a privacy notice via U.S. mail.
Online	<ul style="list-style-type: none"> • Any Web-based form 	<ul style="list-style-type: none"> • For employees or contractors, a privacy notice that meets the content requirements specified in this chapter must be available on screen near where data are 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		<ul style="list-style-type: none"> • 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.

Appendix I. Measurement/Verification Matrix

Responsible Party	Requirement	Measure	Frequency	Party with Measure Responsibility
Application Owner	Log and verify all computer-readable data extracts from databases holding PII and extracts erasure within 90 days.	Spot sample as part of an annual review conducted by the NASA OCIO.	Annual	NASA OCIO
Application & System Owner	Ensure that PII for individuals is protected.	As part of its C&A process, the NASA OCIO will verify compliance via an annual sampling of IPTAs and PIAs will be accomplished by the NASA OCIO of completed IPTAs and PIAs to verify accurate reflection of the data being collected and appropriateness of system controls.	Annual	NASA OCIO
System Owner	Ensure that system meets requirements in this NPR for remote access of PII.	As part of an annual review, spot sample systems to ensure they: <ul style="list-style-type: none"> • Only allow remote access to system PII via two-factor authentication. • Employ a "time-out" function for remote access, requiring user reauthentication after 30 minutes of inactivity. 	Annual	NASA OCIO

SOR System Owner	Log disclosures from the SOR.	Review a sampling of SOR disclosure logs and ensure compliance with approved uses.	Every four years	NASA OCIO
SOR System Owner	Publication of a SORN for new or modified SORs.	Review a sampling of IPTAs for proper citation of an appropriate SORN for applications and systems maintaining IIF that is retrieved by name or personal identifier.	Biennial	NASA OCIO
SOR System Owner	Compliance with SOR requirements in this NPR.	<p>Review a sampling of NASA SORs to verify:</p> <ul style="list-style-type: none"> • Existence of proper contract clauses in contracts for which NASA SORs are managed by contractors. • Functioning procedures to dispose of records in accordance with approved retention schedules. • SOR logs reveal information disclosures only in accordance with approved uses. • Implemented procedures to ensure system record accuracy, relevance, timeliness, and completeness. 	Biennial	NASA OCIO

		<ul style="list-style-type: none"> • Effective presentation of required Privacy Act statements at points of collection. • Proper training of persons involved in the design, development, operation, or maintenance of SORs. 		
NASA OCIO	Review and approve all fully completed PIAs.	Conduct an assessment at the end of each fiscal year to validate that the number of PIAs made public equal the number of PIAs approved.	Annual	NASA OCIO
Users	Encrypt all PII on mobile computers/devices.	Spot sample as part of an annual review.	Annual	NASA OCIO
Web Site Curators	Ensure the proper linking to and posting of Web privacy statements, as required, as they relate to the NASA policy and the sites' use of persistent cookies and collection of PII from the public, including children.	Checks on a sampling of Web sites for appropriate privacy policy statements as prescribed in this NPR.	Annual	NASA OCIO
Web Site RNOs	Ensure reasonable efforts to provide parents or legal guardians of children with notice of the site's information practices and obtain verifiable parental consent to those practices before IIF is collected from a child.	Spot sample as part of a review conducted by the NASA OCIO.	Annual	NASA OCIO

Web Site RNOs	For Web sites employing persistent cookies, obtain prior approval from the NASA CIO to use persistent tracking.		Annual	NASA OCIO
------------------	--	--	--------	-----------