



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1382.1A
Effective Date: July 10, 2013
Expiration Date: July 10,
2018

[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: NASA Privacy Procedural Requirements

Responsible Office: Office of the Chief Information Officer

[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) | [ALL](#) |

Chapter 3 - Privacy Risk Management and Compliance

3.1 Privacy Risk Management and Compliance Overview

3.1.1 The Privacy Risk Management and Compliance chapter ensures NASA's compliance with requirements for the collection, assessment, and notice of PII. Additional information on privacy notice is located in Chapter 6, Privacy Notice and Redress.

3.1.2 NASA is responsible for assessing the PII it collects and notifying individuals of what information is collected, why it is being collected, and how the information will be used. In accordance with the Privacy Act, e-Gov Act, and OMB requirements, NASA uses compliance documentation such as PIAs, and Privacy Act System of Records Notices (SORNs). These tools assist NASA in identifying and reducing the privacy risks related to NASA's activities, notifying the public of privacy impacts, and determining which steps to take to mitigate potential impacts to personal privacy. All NASA applications, information systems, and Web sites shall be reviewed via the Initial Privacy Threshold Analysis (IPTA) process to determine whether or not they require a complete PIA.

3.1.3 NASA Privacy Risk Management and Compliance procedures are governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2 Privacy Risk Management and Compliance Policy

3.2.1 Collecting Personally Identifiable Information

The collection of PII during the course of official government business is permitted as long as: (1) authorized by law, (2) Federal and NASA privacy requirements are satisfied, and (3) is otherwise necessary to a NASA program and/or its associated mission. Specific information on collecting PII is governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.1.1 The SAOP shall:

- a. Limit the collection of PII to that which is legally authorized, consistent with Federal and NASA privacy requirements, and to the minimum extent necessary.
- b. Ensure that PII is collected only when necessary for the proper performance of NASA's functions and mission support.
- c. Conduct annual review activities to reduce or eliminate unnecessary collections of PII.

3.2.1.2 The NASA Privacy Program Manager shall coordinate and direct annual NASA-wide review activities to reduce or eliminate unnecessary collections of PII.

3.2.1.3 The CPM shall:

- a. Work with ISOs to ensure that all PII is maintained with accuracy, relevance, timeliness, and completeness.

b. Coordinate annual review activities at the Center level with ISOs to ensure PII is collected in accordance with this policy and to reduce or eliminate unnecessary collections of PII.

c. Work with ISOs to eliminate the unnecessary use of social security numbers (SSNs).

3.2.1.4 The ISO shall:

a. Eliminate the collection of information if the information is not necessary to a NASA program and/or its associated mission.

b. Ensure that all privacy information is maintained with accuracy, relevance, timeliness, and completeness.

c. Ensure that Privacy Act records are collected and maintained in accordance with NASA Privacy Act policies.

d. Conduct annual review activities to reduce or eliminate unnecessary collections of PII.

e. Avoid the collection of SSNs, in accordance with NPD 1382.17, unless required by statute or some another requirement mandating the use of SSNs.

3.2.2 Privacy Impact Assessments

a. A PIA is a formal process through which NASA analyzes how information is processed by an information system, application, or Web site to ensure that its handling conforms to applicable statutory, regulatory, and policy requirements for privacy information. IIF is information that identifies an individual, directly or indirectly. The PIA is used to determine the risks and effects of collecting, maintaining, and disseminating IIF on members of the public. NASA conducts PIAs under two circumstances: (1) in accordance with Section 208 of the e-Gov Act and NIST SP 800-53, for any new or substantially changed 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); or (2) for a new collection of ten or more members of the public in accordance with the PRA.

b. NASA has developed an assessment process to evaluate the nature of the information to be collected and maintained. Responses in the IPTA lead to the determination of what actions shall be taken to comply with applicable statutes, including whether completion of a PIA is required.

c. A PIA describes the information to be collected; the purpose of the collection (why it is collected and its intended use); with whom the information will be shared; if the information was collected with the consent of the owner - or the owner's parent or guardian, if needed (in accordance with COPPA); how the information will be secured; and whether a SOR is created under the Privacy Act. In addition, the PIA examines and documents the evaluation of protections and alternative processes for handling information to mitigate potential privacy risks. Unless otherwise prohibited, NASA is responsible for posting the PIA publicly.

d. Information Security Controls, NIST SP 800-53 PL-5 is governed at NASA by ITS-HBK-2810.03, Planning and ITS-HBK-1382.03, Risk Management and Compliance.

e. Specific information on how to conduct an IPTA and a PIA: review, approval, publication requirements, and the relationship to the PRA and the Privacy Act are governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.2.1 The SAOP shall:

a. Establish Agency policy, requirements, and process for conducting IPTAs and/or PIAs for new or revised applications and information systems.

b. Assess the impact of technology on privacy and the protection of personal information.

c. Approve all completed PIAs.

3.2.2.2 The Center CIO shall ensure that an IPTA, and as appropriate a PIA, is conducted for every application and information system, including Web sites.

3.2.2.3 The NASA Privacy Program Manager shall:

a. Develop and implement Agency policy, requirements, and processes for conducting IPTAs and PIAs as appropriate, for new or revised applications and information systems.

b. Ensure PIAs are thorough and meet all applicable standards.

c. Ensure that completed PIAs are made publicly available for applications and information systems, including Web sites, which collect and/or maintain IIF on members of the public, consistent with Federal policy.

3.2.2.4 The CPM shall:

a. Assist ISOs in the completion of IPTAs and, as appropriate, PIAs.

- b. Conduct timely reviews of applications and information systems, including Web sites, IPTAs and PIAs to ensure the ISO has addressed adequate protection of privacy and/or Privacy Act information.
- c. Ensure the ISOs update IPTAs and, as appropriate, PIAs.
- d. Conduct annual PIA reviews.

3.2.2.5 The ISO shall:

- a. Ensure that an IPTA is conducted and approved for the applications and information systems, including Web sites, under their purview.
- b. Ensure that a PIA is reviewed and approved, as appropriate for:
 - (1) An information system that collects, maintains, or disseminates IIF from or about members of the public; or
 - (2) An electronic collection of IIF for ten or more individuals, consistent with the PRA.
- c. Ensure that all applications and information systems, including Web sites, following significant modification, conduct a re-evaluation of IPTAs and, as appropriate, PIAs.
- d. Ensure that a PIA is conducted prior to use of a third-party Web site or application.
- e. Review completed PIAs annually to ensure ongoing accuracy.

3.2.3 Privacy Act System of Records Notices

In accordance with the Privacy Act, a SORN is required for each NASA SOR containing information on individuals from which records are retrieved by an individual identifier (i.e., name of the individual or by some unique number, symbol, or other identifier assigned to an individual). In order to meet statutory requirements, a SORN shall be published in the Federal Register prior to any collection or new use of information in a Privacy Act system. Specific information on the review, approval, and publication requirements for a SORN are governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.3.1 The SAOP shall:

- a. Provide guidance on the development and publication of SORNs.
- b. Review and issue all SORNs for publication in the Federal Register.

3.2.3.2 The NASA Privacy Act Officer shall:

- a. Review and revise draft SORNs.
- b. Coordinate the Agency review and the SAOP signature of the SORN for submission to the Federal Register for publication through the NASA Federal Register Liaison Officer.
- c. Coordinate with CPMs in determining whether an existing NASA or other government SORN covers Privacy Act records maintained by NASA.

3.2.3.3 The CPM shall:

- a. Work with ISOs in identifying the need for a Privacy Act SORN.
- b. Assist the ISO in drafting a SORN for publication in the Federal Register, if not already covered under an existing SORN.
- c. Provide the NASA Privacy Act Officer with draft SORNs, as required.
- d. Conduct SORN reviews, as required.
- e. Coordinate the review and approval of new draft SORNs and Privacy Act notice updates with ISOs and the NASA Privacy Act Officer.

3.2.3.4 The ISO shall:

- a. Limit the maintenance of Privacy Act records on individuals that are retrievable by name or other personal identifier to only those instances for which a Privacy Act SORN has been published in the Federal Register.
- b. Draft a SORN for publication in the Federal Register, if not already covered under an existing SORN.
- c. Work with the CPM and the NASA Privacy Act Officer to publish a SORN in the Federal Register.

3.2.4 Privacy Act (e)(3) Statements.

In accordance with the Privacy Act, individuals who are asked to provide information that will be maintained in a

NASA Privacy Act SOR are required at the point of collection to be presented with a Privacy Act 5 U.S.C. § 552(a)(e)(3) Statement (hereinafter referred to as a Privacy Act Statement). The Privacy Act Statement requirement may be accomplished through a standalone paper based statement, a statement on the paper or electronic form, or an electronic statement on a dedicated Web page. Specific information on Privacy Act Statement requirements is governed by ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.4.1 The SAOP shall provide guidance on the use of Privacy Act Statements.

3.2.4.2 The NASA Privacy Act Officer shall work with the CPM to ensure the Privacy Act Statement meets the requirements of the Privacy Act.

3.2.4.3 The CPM shall work with ISOs to ensure the Privacy Act Statement meets the requirements of the Privacy Act.

3.2.4.4 The ISO shall:

a. Ensure that individuals who are asked to provide information to be maintained in a Privacy Act SOR are presented at the point of collection with a Privacy Act Statement that:

(1) Is presented either on the information collection sheet or screen, or via a separate sheet or screen that the individuals can print and retain;

(2) Complies with the requirements outlined in 14 CFR 1212.602; and

(3) Is in a format that the individual may be able to retain in a physical or hard copy.

b. Ensure that new NASA forms or Center forms created for the collection of SOR information provide the correct and specific Privacy Act Statement for that SOR.

3.2.5 Computer Matching Agreements.

In accordance with the Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988, a public notice of the proposed match and the computer matching agreement is required to be published in the Federal Register before NASA can match its data with another Federal entity or state government. Specific information on Computer Matching Agreement requirements governed by is detailed in ITS-HBK-1382.03, Privacy Risk Management and Compliance.

3.2.5.1 The NASA SAOP shall:

a. Establish a Data Integrity Board that is responsible for approving, overseeing, and coordinating the matching program before any ISO may engage in a computer matching program as defined by the Privacy Act.

b. Provide guidance on computer matching agreements.

3.2.5.2 The NASA Privacy Act Officer shall work with the ISO to prepare and publish a notice in the Federal Register at least 30 days in advance of the establishment or revision of a matching program.

3.2.5.3 The ISO shall prepare and publish a notice in the Federal Register at least 30 days in advance of the establishment or revision of a matching program, in coordination with the NASA Privacy Act Officer.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) | [Chapter6](#) |
[Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) |
[AppendixE](#) | [ALL](#) |

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

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
