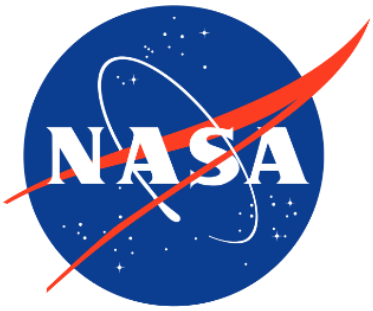
NAII 1382.1
NPR 1382.1

NASA Privacy Program Plan



Privacy Program Plan
National Aeronautics and Space Administration

September 2024

NASA Privacy Program Plan

Effective: 09/30/2024
Expiration: Until Rescinded
Revision #: 1.7

REVISION HISTORY

Revision #	Date	Description of Change	Author/Editor
1.0	10/17/17	Initial Draft	Mike Terry
1.1	10/12/18	Updated to include BRT and SBU sections.	Mike Terry
1.2	10/07/19	Updates to privacy common controls	Mike Terry
1.3	09/15/20	Updates to include RISCS	Stayce Hoult
1.4	09/10/21	Updated to incorporate ITS-HBK- 1382.02-01 goals and objectives	Stayce Hoult
1.5	09/22/2022	Updated privacy controls, policy references and CUI occurrences to correspond with current privacy/CUI posture.	Emmanuel Nyarko
1.6	10/07/2023	Updated document to reflect amended policy alignment consistent with OCIO transformation and Agency-wide role assignment. Additionally, better aligned BRT activities with SOC processes.	CPO Support Team
1.7	09/30/2024	Further updates resulting from OCIO transformation.	CPO Support Team

1. INTRODUCTION

The National Aeronautics and Space Administration (NASA) is committed to protecting all personally identifiable information (PII) it collects from individuals. NASA's goal is to maintain public trust, protect NASA's image, and ensure fairness to individuals who entrust their PII to NASA. This document outlines NASA's plan to fulfill that goal.

NASA's Privacy Program Plan provides an overview of the Agency's Privacy Program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy (SAOP) and other privacy officials, strategic goals, and identifies Privacy controls incorporated in National Institute of Standards and Technology (NIST) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.

NASA requirements for protecting the security of NASA information and information systems are derived from NIST guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems follow NIST guidance in the proper security categorization (Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems), and in the selection and implementation of information security controls (FIPS 200, Minimum Security Requirements for Federal Information and Information Systems), and (NIST 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organization), in a manner consistent with the Risk Management Framework (NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems).

NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information and Information Systems, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.

This document supports implementation of requirements in NPR 1382.1, NASA Privacy Procedural Requirements and NPD 1382.1, NASA Privacy Policy. It also augments NIST guidance with NASA-specific requirements, procedures, and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within the Risk Information Security Compliance System (RISCS) system.

2. PURPOSE

The NASA Privacy Program is aligned with the Cybersecurity and Privacy Division (CSPD) strategic goal for data classification. NASA also aligns its goals with the *Fair Information Practice Principles* found in OMB Circular A-130, *Managing Information as a Strategic Resource.* The SAOP has established the goals identified within this program plan to provide a roadmap for the NASA privacy program as it implements NASA's policies. The NASA Privacy Program goals are:

- To ensure that NASA only collects privacy information that is necessary for the proper performance of a NASA function and has a practical utility (as defined in NPR 1382.1, and ITS-HBK-1382.03-01, *Privacy—Collections, PTAs, and PIAs*.
- To align NASA privacy policy, procedural requirements, and handbooks with Federal requirements.
- To conduct annual reviews of collections of privacy information and reduce or eliminate unnecessary collections.
- To maintain and publish NASA's Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and an accurate and current web privacy policy.
- To maintain and publish privacy notices.
- To provide the public with an opportunity to comment on NASA's privacy policies, to state complaints, and to seek redress.
- To notify members of the public and NASA users of any breach of their personal information collected, maintained, or stored by NASA (regardless of the data format).
- To ensure that Agency Privacy Managers (APMs), Information System Owners (ISOs), information owners, and NASA users are provided with appropriate guidance and support.

2.1 SCOPE

NASA has developed the 1382 and 2810 series Information Technology Handbooks (ITS-HBK) implementing NPD 1382.1, *NASA Privacy Policy*, NPR 1382.1, *NASA Privacy Procedural Requirements* and NPR 2810.7, *Controlled Unclassified Information (CUI)*.

Any non-concurrence, disapproval, denial, or request for deviation from the policy guidance or procedural requirements set forth in this program plan is accompanied with a documented rationale and/or justification to support such decision.

3. POINTS OF CONTACT(S)

For any questions or comments regarding the contents of this document, contact:

Stayce Hoult, NASA Chief Privacy Officer, stayce.d.hoult@nasa.gov.

The point of contact for this document to address and resolve any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with its interpretation.

4. APPLICABILITY

This document applies to NASA Headquarters and NASA Centers. NASA Centers include Component Facilities and Technical and Service Support Centers, such as the Jet Propulsion Laboratory, a Federally Funded Research and Development Center (FFRDC), and other contractors, authorized users, grant recipients, or parties to agreements when specified or referenced in relevant contracts, grants, or agreements.

Compliance with this document is mandatory. Non-compliance may result in the suspension or revocation of access to NASA IT, disciplinary action, as well as civil and criminal penalties.

This document and the policy/procedural guidance contained within remains in full force and effect until such time that the document is formally cancelled, rescinded, or superseded by an updated document.

5. APPLICABLE DOCUMENTS

5.1 FEDERAL LAWS AND REGULATIONS

- National Aeronautics and Space Act, as amended, 51 United States Code (U.S.C.) § 20101 et seq.
- NASA Privacy Act Regulations, 14 CFR Part 1212
- Privacy Act of 1974, as amended, 5 U.S.C. § 552a
- Federal Information Security Management Act (FISMA) of 2014, 44 U.S.C. § 3541 etseq.
- E-Government Act of 2002, as amended, 44 U.S.C. § 3601 et seq.
- Paperwork Reduction Act of 1995 (PRA), 44 U.S.C. § 3501 et seq., as amended
- Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § 6501 et seq., 16 C.F.R part 312
- Social Security Number Fraud Prevention Act of 2017

5.2 OFFICE OF MANAGEMENT AND BUDGET (OMB)

- OMB Circular A-130, *Managing Information as a Strategic Resource*

- OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting,and Publication under the Privacy Act*
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach ofPersonally Identifiable Information*
- OMB Memorandum M-17-09, *Management of Federal High Value Assets*
- OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites andDigital Services*
- OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officialsfor Privacy*

5.1. NASA POLICIES AND HANDBOOKS

- NPR 1382, *NASA Privacy Procedural Requirements*
- NPR 2810.7, *Controlled Unclassified Information (CUI)*
- ITS-HBK-1382.03-01, *Privacy - Collections, PTAs, and PIAs*
- ITS-HBK-1382-04-01, *Privacy and Cybersecurity*
- ITS-HBK-1382- 05-01, *Privacy Incident Response and Management: Breach Response Team Checklist*

6. ROLES AND RESPONSIBILITIES

NASA dedicates both human and technical resources to its privacy program. The human resources dedicated are the SAOP, Chief Privacy Officer, Privacy Act Officer, Paperwork Reduction Act Clearance Officer, and Agency Privacy Managers. Additional support staff, either civil servants or contractors, may be assigned in support of NASA's Privacy Program as required.

The Risk Information Security Compliance System (RISCS) is an automated system NASA uses to meet Privacy requirements along with several other Privacy related compliance and risk management activities. An initial Privacy Threshold Analysis (PTA) is performed in RISCS for every information collection. During the initial PTA process NASA privacy professionals assess the privacy risks associated with a collection of PII and identify associated regulatory compliance requirements. Through a series of questions, stakeholders are informed of the need to:

- complete a PIA,
- indicate, initiate, or modify a SOR,
- request clearance from Office of Management and Budget (OMB) for collections subject to the Paperwork Reduction Act (PRA).

NASA also maintains its Master Privacy Information Inventory (MPII) in RISCS.

NASA adheres to guidance from both the NIST Privacy Framework and the NIST Risk Management Framework so that privacy and cybersecurity teams collaborate on shared objectives.

6.1 SENIOR AGENCY OFFICIAL FOR PRIVACY (SAOP)

The NASA Administrator delegates to the SAOP the overall responsibility and accountability for ensuring NASA's implementation of personal information protections, including the Agency's full compliance with Federal laws, regulations, and policies relating to privacy information. The SAOP designates the Chief Privacy Officer and the Privacy Act Officer and delegates various privacy management responsibilities to each role.

6.2 CHIEF PRIVACY OFFICER (CPO)

The CPO performs oversight, governance, training, and implementation responsibilities for privacy activities on behalf of the SAOP. This includes responding to external inquiries, ensuring compliance with Federal law and regulations, developing privacy policies, and providing counsel to the SAOP or other NASA officials regarding privacy issues.

6.3 PRIVACY ACT OFFICER (PAO)

The Privacy Act Officer (PAO) ensures compliance with Privacy Act requirements. This includes ensuring Systems of Records Notices are published in the Federal Register, initiating regular System of Records reviews, and maintaining effective communication with Agency Privacy Managers and other NASA personnel regarding Privacy Act issues.

6.4 PAPERWORK REDUCTION ACT CLEARANCE OFFICER

NASA Paperwork Reduction Act (PRA) Clearance Officer implements the OPM information collection process to ensure OPM information collection requests meet OMB requirements. Under Paperwork Reduction Act, the collection owners should work with the NASA PRA Clearance Officer to obtain OMB authorization for the collection.

6.5 AGENCY PRIVACY MANAGERS (APMs)

Agency Privacy Managers directly support the CPO and serves as the foremost expert and consultant on all NASA privacy matters, including overseeing, managing, and implementing NASA privacy policies and procedural requirements Agency-wide. For a full listing of all roles and responsibilities refer to NPD 1382.1 and NPR 1382.1.

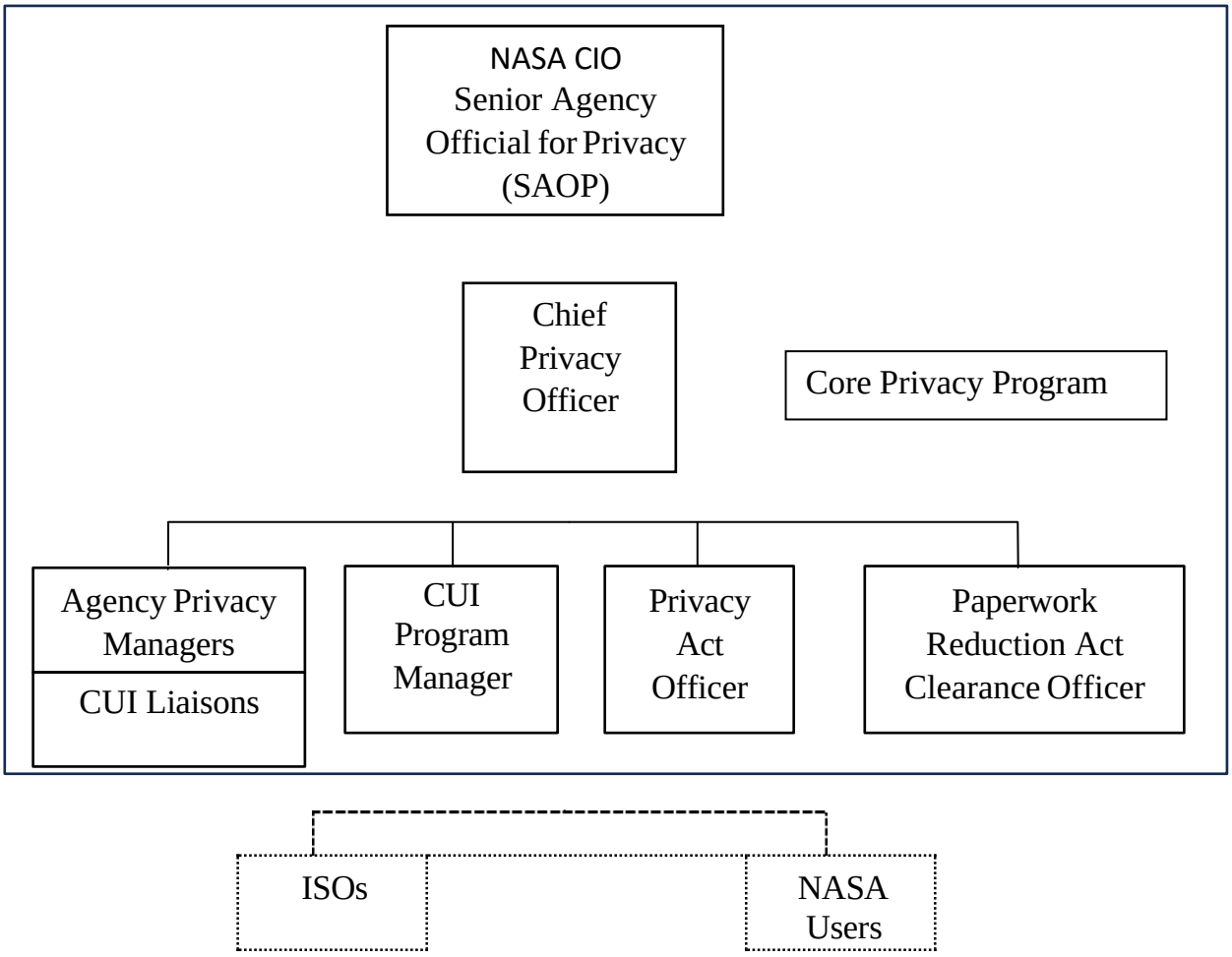
6.6 CUI PROGRAM MANAGER (CUI PM)

The CUI Program Manager manages the day-to-day operations of NASA’s CUI Program, as directed by the CUI SAO

7. PRIVACY PROGRAM MANAGEMENT

The SAOP designates NASA's Chief Privacy Officer and Privacy Act Officer. The CPO designates an APM as well as the CUI Program Manager since the CUI program is a component of the Privacy Program. Figure 1 illustrates the NASA Privacy Program structure.

Figure 1, NASA Privacy Program



8. BREACH RESPONSE

NASA responds to both confirmed and suspected breaches of PII. NASA reports to applicable authorities when a confirmed breach of PII meets the threshold outlined in the handbooks associated with Chapter 6 of NPR 1382.1, *NASA Privacy Procedural Requirements*. A Breach Response Team

(BRT) is convened upon confirmation of a breach (usually within 24 hours). The BRT:

- Analyzes risk associated with the breach and determines identity protection services in accordance with OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, NASA policies and guidelines.
- Apprises NASA leadership.
- Recommends remediation.
- Drafts breach notification letters, Frequently Asked Questions (FAQs) etc.

Core members of the BRT include the CPO/APM, the SAISO/dSAISO, and an Agency Incident Response Manager (IRM) or their designees. Membership of the BRT differs depending on the type and complexity of a breach. Additional members may include:

- Privacy Act Officer
- OCIO staff
- Center Chief Information Officer
- Center Chief Information Security Officer
- Office of the Inspector General (involved where there is a suspected criminal intent)
- Office of the General Counsel (for review of any breach notification determinations and materials)
- Office of Communications (for review of any breach notification materials related to media outlets)
- Information System Owner(s)
- Contracting Officer or Representative
- Human Resources Employee Relations Representative
- Subject Matter Experts, as needed

If a privacy breach impacts multiple Centers, this list will be expanded appropriately.

NASA BRT activities are governed by NPR 1382.1, NASA Privacy Procedural Requirements and ITS-HBK1382,05-01, *Privacy Incident Response and Management: Breach Response Team Checklist.*

9. CONTROL IMPLEMENTATION

NASA has implemented the privacy controls found in National Institute of Standards and Technology (NIST) 800-53 Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*. A full listing of NASA's implementation of the NIST 800-53 Rev.5 can be found in NASA-SPEC-2661, *Controls and NASA-*

SPEC- 2661.ODVr5. Figure 2 specifies privacy controls as outlined in ITS-HBK-04-01, *Privacy and Cybersecurity Controls Framework* implemented and/or planned at NASA for privacy risk management.

Figure 2, NASA Privacy Controls

NIST Control #	Control and Control Enhancement Name
AC-01*	Policy and Procedures
AC-03(14)	Access Enforcement | Individual Access
AC-21	Information Sharing
AT-01 *	Policy and Procedures
AT-02 *	Literacy Training and Awareness
AT-03 *	Role-based Training
AT-03(05)	Role-based Training | Processing PII
AT-04	Training Records
AU-01 *	Policy and Procedures
AU-02	Event Logging
AU-03(03)	Content of Audit Records | Limit PII Elements
AU-11	Audit Record Retention
CA-01 *	Policy and Procedures
CA-02 *	Control Assessments
CA-05 **	Plan of Action and Milestones
CA-06 **	Authorization
CA-07 **	Continuous Monitoring
CA-07(04)	Continuous Monitoring |Risk Monitoring
CM-01 *	Policy and Procedures
CM-04 *	Impact Analyses
IR-01 *	Policy and Procedures
IR-02	Incident Response Training
IR-02(03)	Incident Response Training | Breach

IR-03	Incident Response Testing
IR-04	Incident Handling
IR-05	Incident Monitoring
IR-06 **	Incident Reporting
IR-07	Incident Response Assistance
IR-08	Incident Response Plan

IR-08(01)	Incident Response Plan | Breaches
MP-01*	Policy and Procedures
MP-06	Media Sanitization
PE-08(03)	Visitor Access Records | Limit PIIElements
PL-01 *	Policy and Procedures
PL-02 *	System Security and Privacy Plans
PL-04 **	Rules of Behavior
PL-04(01)	Rules of Behavior | Social Media and External Site/application Usage Restrictions
PL-08	Security and Privacy Architectures
PL-09	Central Management
PM-03	Information Security and Privacy Resources
PM-04	Plan of Action and Milestones Process
PM-05(01)	System Inventory | Inventory of PII
PM-06	Measures of Performance
PM-07	Enterprise Architecture
PM-08	Critical Infrastructure Plan
PM-09	Risk Management Strategy
PM-10	Authorization Process
PM-11	Mission and Business Process Definition
PM-13	Security and Privacy Workforce
PM-14	Testing, Training, and Monitoring
PM-17	Protecting CUI on External Systems
PM-18	Privacy Program Plan
PM-19	Privacy Program Leadership Role
PM-20	Dissemination of privacy Program information

PM-20(01)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services
PM-21	Accounting of Disclosures
PM-22	PIIQuality Management
PM-24	Data Integrity Board
PM-25	Minimization of PII Used in Testing, Training, and Research
PM-26	Complaint Management
PM-27	Privacy Reporting
PM-28	Risk Framing
PM-31	Continuous Monitoring Strategy
PS-06	Access Agreements
PT-01 *	Policy and Procedures
PT-02	Authority to Process PII
PT-03	PII Processing Purposes
PT-04	Consent
PT-05	Privacy Notice
PT-05(01)	Privacy Notice | Just-in-time Notice
PT-05(02)	Privacy Notice | Privacy Act Statements
PT-06	System Of Records Notice (SORN)
PT-06(01)	SORN | Routine Uses
PT-06(02)	SORN | Exemption Rules
PT-07	Specific Categories of PII
PT-07(01)	Specific Categories of PII | SSNs
PT-07(02)	Specific Categories of PII | First Amendment Information
PT-08	Computer Matching Requirements
RA-01*	Policy and Procedures
RA-03*	Risk Assessment
RA-07	Risk Response
RA-08**	Privacy Impact Assessments
SA-01*	Policy and Procedures
SA-02 *	Allocation of Resources
SA-03	System Development Life Cycle
SA-04	Acquisition Process

SA-08(33)	Security and Privacy Engineering Principles | Minimization
SA-09	External System Services
SA-11	Developer Testing and Evaluation
SC-07(24)	Boundary Protection | PII
SI-01*	Policy and Procedures
SI-12	Information Management and Retention
SI-12(01)	Information Management and Retention | Limit PIIElements
SI-12(02)	Information Management and Retention | Minimize PII in Testing, Training and Research
SI-12(03)	Information Management and Retention |Information Disposal
SI-18	PIIQuality Operations
SI-18(04)	PII Quality Operations | Individual Requests
SI-18(05)	PII Quality Operations | Notice of Correction or Deletion
SI-19	De-identification

***NASA Critical Control, ** Federally Mandated Critical Control**

10. CONTROLLED UNCLASSIFIED INFORMATION

Requirements for designating, accessing, storing, disseminating, decontrolling, and destroying PII which require special handling are commensurate with Executive Order (EO) 13556, 32 CFR Part 2002, and NPR 2810.7, *Controlled Unclassified Information*. For example:

Sharing CUI information only with NASA users who have a "lawful government purpose" in connection with their job assignment.

- Encrypting CUI information in transit and at rest using a FIPS 140-2 certified solution.
- Ensuring CUI is secured when unattended.
- Shipping or mailing CUI should be marked as " Open by Addressee Only" and avoid CUI markings on outside package/envelope.

11. AWARENESS AND TRAINING

Prior to gaining access to NASA information and information systems NASA stakeholders are required to take Cybersecurity and Privacy Awareness Trainings (CPAT) which instructs users on how to report suspected/confirmed privacy related incidents, and consequences for violating Federal and NASA policies. Additionally, users acknowledge NASA Rules of Behavior (NASA RoB)which

provide specific responsibilities and expected behavior for all NASA Information Technology Systems per:

- Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource, Appendix Ill, paragraph 3a(2)(a),*
- NPD 2810, *NASA Information Security Policy*, and
- NPD 2540, *Acceptable Use of Government Furnished Information Technology Equipmentand Resources.*

12. ACRONYMS

Acronym	Definition
BRT	Breach Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
APM	Agency Privacy Manager
CSPD	Cybersecurity and Privacy Division
CUI	Controlled Unclassified Information
FIPS	Federal Information Processing Standards
ISO	Information System Owner
ITS	Information Technology Security
ITSATC	Information Technology Security Awareness and Training Center
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
RISCS	Risk Information Security Compliance System
SAOP	Senior Agency Official for Privacy
SORN	System of Records Notice
SP	Special Publications

13. GLOSSARY

Agency Privacy Manager (APM)	The principal advisor to the Center Director, Center CIO, Center CISO, and ISOs on matters pertaining to privacy and acts as Privacy Act liaison with the NASA Privacy Act Officer. Responsible for the day-to-day operations of the Agency Privacy program. (NPR 1382.1)
Chief Information Security Officer (CISO)	The principal advisor to the Senior Agency Information Security Officer, Center Chief Information Officer, and senior Center officials on matters pertaining to information security. (NPR 2810.1)
Information System Owners (ISOs)	The principal advisor to the Center Chief Information Security Officer (CISO) on matters pertaining to specific information systems. (NPR 2810.1)
NASA User	Any explicitly authorized patron of a NASA information system. (NPR 2810.1)
Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (OMB Circular A-130, OMB M17-12, OMB M- 10-23)
Privacy Impact Assessment (PIA)	An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis. (OMB Circular A-130, Section 208 of the E-Government Act of 2002)
Senior Agency Official for Privacy (SAOP)	The senior official, designated by the head of each agency, who has agency- wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy- making role in the agency's development and evaluation of legislative, regulatory, and other policyproposals. (OMB Circular A-130, OMB M-16-24)

System of Records Notice (SORN)	The notice(s) published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in [OMB Circular A-108].

STAYCE HARRIS HOULT

Digitally signed by STAYCE HARRIS HOULT
Date: 2024.10.16 14:03:49 -05'00'

Stayce D. Hoult
NASA Chief Privacy Officer