NAII 1382.2
NPR 1382.1

Policy for Privacy Continuous Monitoring National Aeronautics and Space Administration

November 5, 2024

Revision History

Revision #	Date	Description of Change	Author/Editor
1.0	10/25/2023	Updated to reflect modified policy and OCIO transformation	CPO Support Team
1.1	9/27/2024	Annual review and revalidation	CPO Support Team

Table of Contents

1. OVERVIEW

This document catalogues National Aeronautics and Space Administration (NASA) policies for Privacy Continuous Monitoring and outlines the Agency's risk management activities, implementation, and assessment of privacy controls implemented at the Agency across all risk management tiers and ensure they are constantly monitored.[1] Additionally, per Office and Management ad Budget (OMB) Circular A-130, the SAOP develops and maintains a privacy continuous monitoring strategy, a formal document that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. [2] It is designed to consolidate all available policies. These polices allow NASA to maintain public trust, protect its image, and ensure fairness to individuals who entrust their Personally Identifiable Information (PII) to NASA.

The Agency adheres to and conducts an ongoing assessment of privacy set out in the OMB Circular A-130, "Privacy continuous monitoring" means maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.[3] NASA's overarching policy enshrined in NPR 1382.1, NASA Privacy Procedural Requirements integrates privacy controls across multiple control families in NIST SP 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations in the assessment, authorization, and continuous monitoring. Additionally, NASA has a dedicated technical handbook, Step 6, Monitor Policy, that relies heavily on concepts outlined in the latest version of NIST SP 800-37, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

NASA conducts and documents privacy control assessments consistent with frequency defined in its policies, handbooks, privacy program and plans on Information Security Continuous Monitoring (ISCM) and Privacy Continuous Monitoring (PCM)[4]. For NASA, this means reviewing privacy risks at the earliest planning and development stages of information systems and continuously monitoring privacy risks throughout the information lifecycle.

2. PRIVACY ACTIVITIES

2.1 PII COLLECTION AUTHORITY AND PURPOSE (PT-02, PT-03)

These controls ensure that NASA:

(i) Identifies the legal bases that authorizes a PII collection or activity potentially impacting privacy.

(ii) Specifies in Agency notices the purpose(s) for which PIIis collected; Restricts the processing of PII to only that which is authorized; and

(iii) Monitors changes in processing PII to ensure they comply with NASAlegal requirements.

Implementation: NASA only permits the collection and processing of PII when the activity is permitted under an established legal authority and required for the performance of a NASA function or mission. This

[1] OMB Circular No. A-130, *On Privacy Continuous Monitoring*, pg. 33.
[2] *Idem*, pg. 82.
[3] *Idem* pg. 34.
[4] NPD 1382, NPD 2810, Privacy control family handbooks in CSET, NASA Privacy Program Plan.

requirement is supported by the Privacy Threshold Analysis (PTA) process, which is completed for all applications and systems, and determines the need to complete a Privacy Impact Assessment (PIA). The purpose of each collection is also identified during the PTA process. All PTAs and PIAs are reviewed and approved by a relevant privacy official, as appropriate, and privacy notices are updated as required. Processes for PTAs and PIAs are governed by NASA Procedural Requirement (NPR) 1382.1, *NASA Privacy Procedural Requirements.*

Assessment Frequency: All NASA information owners and information system owners are required to annually review collections of PII during the review and reduce activity in accordance with IT Security Handbook (ITS-HBK) 1382.03-02, *Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of Social Security Numbers (SSN)*.

2.2 PRIVACY PLAN, GOVERNANCE, AUDIT, ACCOUNTABILITY AND RISK MANAGEMENT (PM-03, PM-18, PM-19, RA-03, RA-08, SA-01, SA-04, SA-09, CA-02)

These controls ensure public confidence through effective governance, monitoring, risk management, and privacy requirements in acquisitions and assessment to demonstrate that NASA complies with applicable privacy protection requirements and is minimizing overall privacy risk.

Implementation : The SAOP has overall responsibility for developing and maintaining the NASA Privacy Program. The SAOP appoints a Chief Privacy Officer (CPO) to perform oversight, governance, training, and implementation responsibilities of privacy activities on behalf of the SAOP. NASA Procedural Requirement (NPR) 1382.1, *NASA Privacy Procedural Requirements* provides an overall governance of the NASA Privacy Program, the Privacy Threshold Analysis (PTA), and Privacy Impact Assessment (PIA) process. A PTA is performed for each collection of information and allows NASA privacy officials to analyze the potential privacy risks associated with the collection. The SAOP provides input to the NASA Capital Planning and Investment Control (CPIC) process to ensure adequate funding is included in NASA's budget requests to the U.S. Congress. System Owners ensure that risk assessments are conducted to determine the likelihood and impact that these risks would have on individuals whose PII is collected, stored, managed, or disseminated by the system.

Assessment Frequency: NASA updates NPR 1382.1, every five (5) years. In addition, all NASA information owners and information system owners are required to annually review collections of PII during the annual review and reduce activity in accordance with ITS-HBK-1382.03-02, *Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN*. NASA implements continuous monitoring activities for security and privacy controls for all systems in keeping with National Institutes of Standards and Technology (NIST) Special Publications (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* and OMB guidance (OMB M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestone*).

2.3 PRIVACY AWARENESS AND TRAINING (AT-01, AT-02, AT-03, PL-04)

These controls ensure that NASA creates and provides all personnel with Cybersecurity and Privacy Awareness Training (CPAT) to ensure they understand their responsibilities, the legal basis for those responsibilities, and NASA expectations for managing privacy information. NASA also creates and provides special role-based training for those responsible for specialized Privacy activities.

Implementation: NASA creates training materials to ensure all personnel understand their privacy responsibilities. The training is provided, and completion details are tracked through the System for Administration, Training, and Educational Resources for NASA (SATERN). Additionally, specialized privacy training is provided for those with specific privacy roles at NASA. Lastly, NASA includes general privacy training requirements for all personnel as part of yearly, mandatory Rules of Behavior (RoB) activities, which all personnel must acknowledge.

Assessment Frequency: All privacy training materials and RoB requirements are reassessed on a yearly basis to ensure that guidance is updated as mandated by NASA leadership or when legal or federal guidance related to privacy activities is updated.

2.4 PRIVACY REPORTING AND DISCLOSURE MANAGEMENT (PM-21, PM-27)

These controls ensure that NASA develops and maintains procedures to accurately account for PII disclosures, maintains record of these disclosures in keeping with federal guidance, develops and disseminates privacy reports, and makes such accounting details available to relevant individuals or organizations upon request.

Implementation: NASA has implemented a Master Privacy Information Inventory (MPII) that is automated within the Risk Information Security Compliance System (RISCS). System, application, and information owners are required by policy established in NPR 1382.1, to update associated PTAs or PIAs within the RISCS, upon any change, which automatically updates the Agency MPII. NASA develops and maintains an accounting of all PII disclosures in keeping with 14 CFR §1212.203 and NPR 1382.1. NASA maintains a record of all disclosures for at least 5 years after the disclosure and makes the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

NASA creates privacy reports in response to internal reporting requirements in keeping with NPR 1382.1 and requests from external federal regulatory bodies in support of compliance validation activities in keeping with ITS- HBK-1382.03-02, *Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN* and Office of Management and Budget guidance.

Assessment Frequency: NASA reviews and updates privacy reports annually in keeping with ITS-HBK-1382.03-02, *Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN*. NASA also provides ad hoc reporting in keeping with Office of Management and Budget Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, when a privacy incident occurs.

2.5 PRIVACY DATA INTEGRITY AND QUALITY (PM-22, SI-18, PM-24, SI-01)

These controls ensure public confidence that any personally identifiable information (PII) collected and maintained by NASA is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

Implementation: NPR 1382.1 requires Agency Privacy Managers (APMs) and information system owners to ensure that PII is maintained with accuracy, relevance, timeliness, and completeness. NASA has automated this process using the RISCS to track, monitor, and report on APMs' and information owners' validation of all PII collections. NASA does not currently have any matching agreements, however, if matching agreements are entered into, a Data Integrity Board will be established, and agreements will

be published at www.nasa.gov/privacy.

Assessment Frequency: All NASA information owners and information system owners are required to annually review collections of PII during the annual review and reduce activity in accordance with ITS-HBK-1382.03-02, *Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN.*

2.6 PII MINIMIZATION, RETENTION AND DISPOSAL (SA-08(33), PM-05(01), SI-12(01), MP-06, SI- 12, SI-12(03), PM-25, SI-12(02))

These controls ensure NASA implements data minimization and retention requirementsto collect, use, and retain only personally identifiable information (PII) that is relevant and necessary for the purpose for which it was originally collected. NASA must retain the PII for as long as necessary to fulfill the intended purpose(s) for which it was collected and meet National Archives and Records Administration (NARA)-approved record retention schedule(s). When privacy information is no longer required, NASA follows NIST, National Security Agency (NSA) guidance, and NASA's guidance defined in ITS-HBK- 2810.11-2C, Media-Protection-and-Sanitization, for sanitization of the data.

Implementation: NASA permits the collection of PII only when it is legally authorized and when necessary for the proper performance of NASA's functions or mission. This requirement is part of the PTA prerequisite to be completed prior to the collection of any information, regardless of format, and updated any time a significant change occurs to the collection or instrumentality. Additionally, NASA regularly reviews PII holdings and reduces unnecessary collections of PII in accordance with established Federal requirements.

NASA's policy requirements are provided in NPR 1382.1 and ITS HBK-1382.03-02, *Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN.* NASA applies ITS-HBK- 2810.11-2C, *Media Protection and Sanitization* to sanitize data when it no longer needs privacy-related information. NASA has implemented a Master Privacy Information Inventory (MPII) that is automated within the RISCS. System, application, and information owners are required by policy established in NPR 1382.1, to update associated PTAs or PIAs within the RISCS, upon any change, which automatically updates the Agency MPII.

Assessment Frequency: NASA Information Owners and Information System Owners review collection of PII during the review and reduce activity in accordance with ITS- HBK-1382.03-02, *Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN.* NASA also reviews System of Records Notice (SORN) disposal policies and practices every two (2) years in accordance with ITS-HBK-NPR 1382.1.

2.7 PRIVACY CONSENT, ACCESS, MANAGEMENT AND REDRESS (PT-04, AC-01, AC-03(14), PM-20, PT-05, PT-06, PM-22, SI-18, SI-18(04), SI-18(05), PM-26)

These controls ensure that individuals are active participants in the decision-making process regarding the collection and use of their personally identifiable information (PII). Individuals are provided access to their PII and have the ability to correct or amend their PII as appropriate. The controls in these families enhance public confidence in organizational decisions made based on the information collection containing PII.

Implementation: The NASA process for providing individual participation and redress is found in NPR 1382.1. NASA provides consent information within the general privacy notice or Privacy Act notice, and

specific consent notices associated with each collection of PII. NPR 1382.1 and ITS-HBK- 1382.06-01*, Privacy Notice and Redress — Web Privacy and Written Notice, Complaints, Access, and Redress* permits individual access to PII or Privacy Act records and allows individuals to correct any inaccuracies. NASA has a complaint process that is documented in NPR 1382.1 and in ITS-HBK-1382.06-01. NASA also publishes privacy program information at www.nasa.gov/privacy.

Assessment Frequency: NASA reviews Systems of Records Notices (SORNs) every two (2) years in accordance with NPR 1382.1.

2.8 PII INVENTORY AND INCIDENT RESPONSE (PM-05(01), IR-08, IR-08(01))

These controls ensure that technical, physical, and administrative safeguards are in place to protect PII that NASA collects or maintains against the loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in these families are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework guidance.

Implementation: NASA implements a Master Privacy Information Inventory (MPII) that is automated within the RISCS. System, application, and information owners are required by policy established in NPR 1382.1 to update associated PTAs or PIAs within the RISCS tool, upon any change, which automatically updates to the Agency MPII.

Assessment Frequency: NPR 1382.1 requires Agency Privacy Mangers to continuously update the MPII. In addition, ITS- HBK-1382- 05-01, *Privacy Incident Response and Management: Breach Response Team Checklist* is updated annually.

2.9. PRIVACY NOTICE AND DISSEMINATION (PT-05, PT-05(01), PT-05(02), PT-06, PM-20)

These controls ensure that NASA provides public notice of its information collection practices and the privacy impact of Agency programs and activities as well as clear guidance explaining under what circumstances privacy information may be disseminated.

Implementation: NASA has a general privacy notice available on all public websites and provides specific notice on systems where PII is being collected. The maintenance and use of these notices are governed by NPR 1382.1. NASA regularly publishes Systems of Record Notices (SORNs) for systems containing information subject to the Privacy Act of 1974 and OMB guidance that meet the "who, what, why, and how" requirements, and ensures that they are kept up to date. NASA includes Privacy Act Statements on all forms and collection points that gather PII to be stored in a Privacy Act System of Records (SOR), or on a separate form that can be retained. NASA policy and procedure governing this aspect of the privacy program is contained in NPR 1382.1. NASA also publishes privacy program information at www.nasa.gov/privacy.

Assessment Frequency: NASA reviews its Agency web privacy compliance annually and Systems of Records Notices (SORNs) every two (2) years in accordance with NPR 1382.1.

2.10 PII USE AND LIMITATIONS (PT-03, AC-21, AT-03(05), AU-02, PT-02)

These controls ensure that NASA only uses personally identifiable information (PII)as specified in its public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in these family controls ensures the use of PII in the manner for which it is collected.

Implementation: NASA only permits the collection of the minimum PII legally authorized and necessary for the proper performance of NASA's functions or mission The PTA and PIA process is used to ensure that uses and collections of PII are within the scope of NASA's authority to collect and state whether PII will be shared with third parties. NASA also trains its users on the authorized collection and use of PII. NASA policy is found in NPD 1382.17, *NASA Privacy Policy*, and guidance regarding internal use is found in NPR 1382.1.

Assessment Frequency: All NASA information owners and information system owners are required to annually review collections of PII during the review and reduce activity in accordance with ITS-HBK-1382.03-02, *Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN.* NASA also reviews PIAs annually and its Privacy Act routine use disclosures every four (4) years in accordance with NPR 1382.1.

2.11 ACRONYMS

Acronym	Definition
APM	Agency Privacy Manager
CPAT	Cybersecurity and Privacy Awareness Training
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
ISCM	Information Security Continuous Monitoring
ITS-HBK	Information Technology Security Handbook
MPII	Master Privacy Information Inventory
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PCM	Privacy Continuous Monitoring
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
RISCS	Risk Information Security Compliance System
RoB	Rules of Behavior
SAOP	Senior Agency Official for Privacy
SATERN	System for Administration, Training, and Educational Resources for NASA
SOR	System of Records
SORN	System of Records Notice
SSN	Social Security Number

STAYCE HARRIS HOULT

Digitally signed by STAYCE HARRIS HOULT
Date: 2024.10.16 14:06:19 -05'00'

Stayce D. Houlte
NASA Chief Privacy Officer