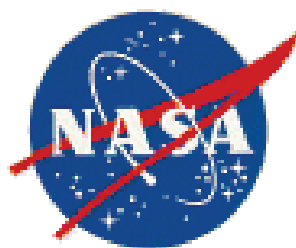




INFORMATION TECHNOLOGY SECURITY HANDBOOK

PRIVACY ACCOUNTABILITY

EFFECTIVE DATE: NOVEMBER 19, 2018



**COMPLIANCE WITH THE POLICIES, PROCEDURES, AND PROCESSES IN THIS
HANDBOOK IS MANDATORY**

Table of Contents

Table of Contents	2
Change History	3
1 Introduction	4
1.1 Purpose	5
1.2 Scope	5
1.3 Point(s) of Contact for this Handbook	6
1.4 Applicable Documents	6
2 Internal Accountability.....	6
2.1 Roles and Responsibilities	6
2.2 Internal Reporting Structure	8
3 External Accountability	8
3.1 Roles and Responsibilities	8
3.2 Mandated Reviews.....	9
Appendix A: Acronyms	11
Appendix B: Glossary	12

Distribution:
NODIS



**Associate Chief Information Officer for
Cybersecurity and Privacy**

Change History

Version	Date	Change Description
1.0	08/28/2012	Initial draft
1.1	08/01/2015	Reviewed by Center CISO's and received signature and approval from SAISO
1.2	11/19/2018	Minor revisions. Reviewed by privacy personnel at the center and agency level.

1 Introduction

National Aeronautics and Space Administration (NASA) requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall 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 Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems and Organizations*), 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 Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.

NPR 1382.1, NASA Privacy Procedural Requirements, designates this handbook as a guide for Chapter 8 of the NPR.

This handbook supports implementation of requirements in *NPD 1382.17, NASA Privacy Policy and NPR 1382.1, NASA Privacy Procedural Requirements*. 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.

1.1 Purpose

NASA is committed to protecting all personally identifiable information (PII) that NASA collects, uses, maintains, and disseminates in furtherance of a NASA program or mission. In order to ensure that the Agency is meeting NASA and Federal requirements for protecting PII, this handbook outlines both the internal (within NASA) and external (outside of NASA) accountability processes and requirements. This handbook outlines NASA's continuous monitoring of the privacy program at the Center and Agency level – accomplished through regular health checks of the privacy program. Specifically, this handbook addresses internal and external reporting requirements and mandated reviews, which is one mechanism the Senior Agency Official for Privacy (SAOP) uses to assess the health of the overall NASA privacy program.

- **Internal Accountability:** Internal accountability refers to reporting that is internal to NASA, such as Centers reporting to the Agency on privacy related inquiries. In order to ensure the continued accuracy of the privacy program health analysis, the Center Privacy Manager (CPM) validates that the Center's master privacy information inventory (MPII), within the Privacy & Controlled Unclassified Information (CUI) Assessment Tool (PCAT), is accurate and complete.
- **External Accountability:** External accountability refers to reporting to entities outside of NASA, such as the Office of Management and Budget (OMB) or the Government Accountability Office (GAO). External accountability is also focused on the mandated privacy reviews that must be conducted each year to ensure compliance with Federal Information Security Modernization Act (FISMA) reporting, as well as NASA's compliance with reviews mandated by the Privacy Act, the E-Government Act, and OMB Circular A-130.

1.2 Scope

This handbook supplements the requirements in Chapter 8 of NPR 1382.1, *NASA Privacy Procedural Requirements*.

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

If a handbook has or refers to an "expiration date" such date is tantamount to a "review date" for the handbook. This handbook and the policy/procedural guidance contained within remains in full force and effect until such time that the handbook is formally cancelled, rescinded or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the policy guidance or procedural requirements set forth in this handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this handbook, in coordination with the CPM to review and validate for the record.

1.3 Point(s) of Contact for this Handbook

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

- NASA Chief Privacy Officer

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 interpretation shall be elevated to the NASA CSPD, in coordination with the CPM, and directed to the attention of the point of contact for this particular handbook to address and resolve.

1.4 Applicable Documents

Federal Law

- *The E-Government Act of 2002, as amended, 44 U.S.C. §§ 101 et seq.*
- *Privacy Act of 1974, as amended, 5 U.S.C. § 552a*

Office of Management and Budget (OMB)

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

National Aeronautics and Space Administration (NASA)

- *NPD 1382.17, NASA Privacy Policy*
- *NPR 1382.1, NASA Privacy Procedural Requirements*
- *ITS-HBK-1382.05-01, Privacy Incident Response and Management*
- *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
- *ITS-HBK-2810.09-02, Incident Response and Management: NASA Information Security Incident Management*

Cancellations, Updates, Consolidations

- *None*

2 Internal Accountability

Internal reporting requirements provide the SAOP with an overview of the health of the privacy program. Note that internal reporting requirements related to the NASA user's responsibility for reporting to the Security Operations Center (SOC) are outlined within ITS-HBK-2810.09-02 and ITS-HBK-1382.05-01.

2.1 Roles and Responsibilities

Agency-Wide

- *NASA Chief Privacy Officer (CPO)*
 - Provide the SAOP with an overview of the health of the privacy program, as requested by the SAOP.

Center Level

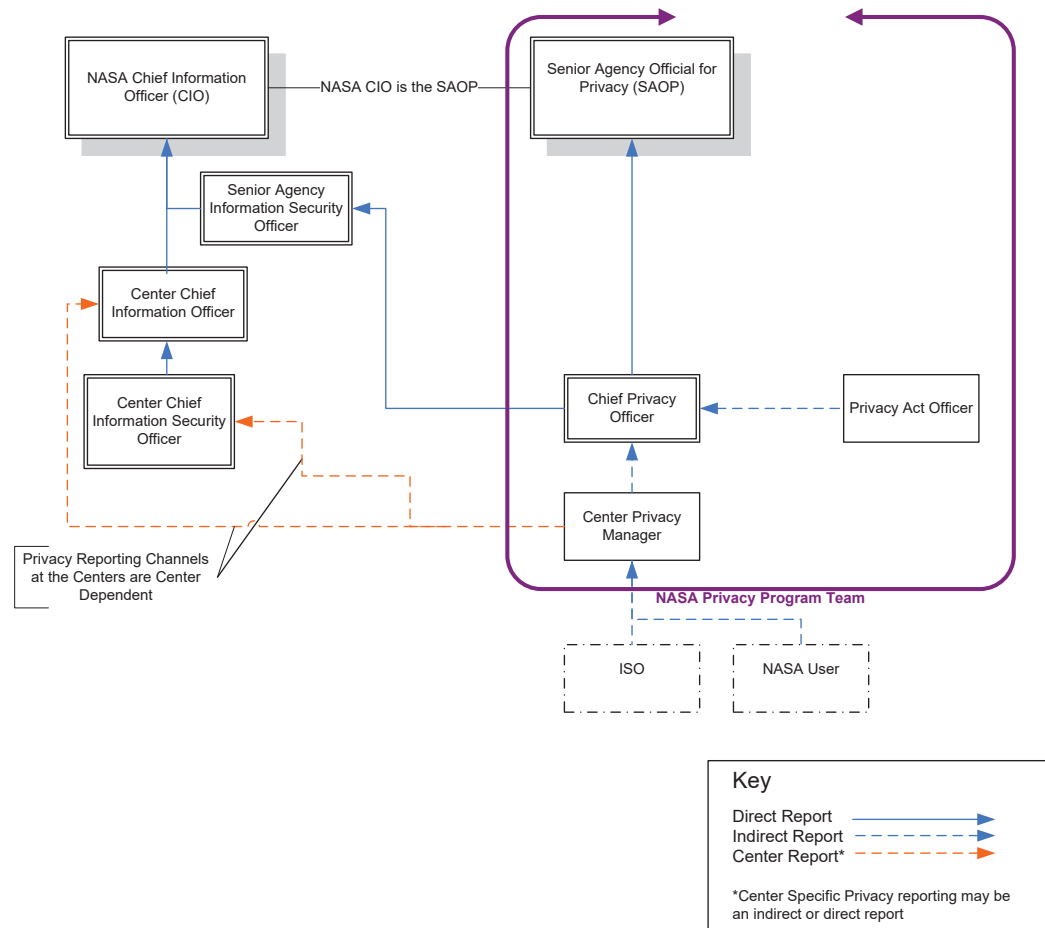
- *Center Privacy Manager (CPM)*
 - Provide monthly updates to the NASA Chief Privacy Officer on the health of the Center privacy program.
 - This may be done via the monthly Video Teleconferencing System (ViTS) meeting or on an individual basis.
 - If there is a privacy breach, violation, or other issue requiring notification to the NASA SOC, the Chief Privacy Officer shall be notified without undue delay (but no later than 48 hours after discovery).
 - Update the MPII within the PCAT to ensure that it is current and accurate at all times.
 - Follow reporting procedures for Privacy Act violations in accordance with Center policy.

Information System Level

- *Information System Owner (ISO)*
 - Ensure that information collected in their information system is documented in PCAT
 - Ensure that data entered into PCAT is accurate to ensure that the MPII is current and accurate at all times.

2.2 Internal Reporting Structure

The internal reporting structure for privacy is illustrated in the figure below:



3 External Accountability

External reporting is essential to validate that NASA is compliant with Federal and NASA requirements.

3.1 Roles and Responsibilities

Agency-Wide

- **Senior Agency Official for Privacy (SAOP)**
 - Ensure that Reviews mandated by the Privacy Act, the E-Government Act, and OMB Circular A-130 are conducted at the frequency prescribed in Table 1, *Mandated Reviews Overview and Frequency*.
- **NASA Chief Privacy Officer (CPO)**
 - Track the completion of mandated reviews for inclusion, as appropriate, within the annual SAOP FIMSA Report.
 - Ensure web privacy policy reviews are conducted at the frequency prescribed in Table 1, *Mandated Reviews Overview and Frequency*.

- *The Privacy Act Officer*
 - Coordinate the mandated Privacy Act reviews outlined in Table 1, *Mandated Reviews Overview and Frequency*. Privacy Act reviews include: matching programs, contracts, recordkeeping practices, and Privacy Act training.
 - The reviews shall be conducted by the end of the Quarter 3 of each Fiscal Year (FY) at the frequency identified in Table 1, *Mandated Reviews Overview and Frequency*.

Center Level

- *Center Privacy Manager (CPM)*
 - Work with the Privacy Act Officer in conducting mandated reviews outlined in Table 1, *Mandated Reviews Overview and Frequency*.
 - Provide any relevant external reporting information to the NASA Chief Privacy Officer as requested and by the end of Quarter 3 of the Fiscal Year.
 - Review Center PII holdings in accordance with ITS-HBK 1382.03-02, Privacy Risk Management and Compliance: Annual Reporting Procedures for Reviewing and Reducing Personally Identifiable Information (PII) and Eliminating the Unnecessary Use of Social Security Numbers (SSN), at the frequency identified in Table 1, *Mandated Reviews Overview and Frequency*.
 - Review PIAs at their center at the frequency identified in Table 1, *Mandated Reviews Overview and Frequency*.

3.2 Mandated Reviews

Type of Review	Frequency	Brief Description	Year Review Required
Matching Programs	Annually	Review each matching program in which the Agency has participated. Where possible, reduce the amount or type of PII collected to the bare minimum necessary.	Annually
Review and Reduce PII	Annually	Review all personally identifiable information (PII) holdings	Annually
Privacy Impact Assessments	Annually	Review the number of completed Privacy Impact Assessments (PIAs) to number of posted PIA summaries.	Annually
Website Privacy Compliance	Annually	Review NASA websites to ensure that they have posted links to the NASA privacy page	Annually
Contracts	Every 2 Years	Review random sample of Agency contracts that provide for the maintenance of a System of Record (SOR) on behalf of NASA.	2018, 2020, 2022, 2024

Type of Review	Frequency	Brief Description	Year Review Required
Recordkeeping Practices	Every 2 Years	Review System of Records Notice (SORN) disposal policies and practices, including the maintenance of automated records.	2019, 2021, 2023, 2025
Privacy Act Training	Every 2 Years	Review training practices to ensure that all Agency personnel are familiar with Privacy Act requirements.	2019, 2021, 2023, 2025
Violations	Every 2 Years	Review actions of Agency personnel that have resulted in the Agency or the employee being found liable or guilty.	2019, 2021, 2023, 2025
Systems of Records Notices	Every 2 Years	Review each SORN for accuracy and appropriateness.	2019, 2021, 2023, 2025
Routine Use Disclosures	Every 4 Years	Review the disclosure practice associated with each SOR.	2021, 2025, 2029, 2032
Exemption of Systems of Records	Every 4 Years	Review each SOR for which the Agency has identified exemption rules.	2021, 2025, 2029, 2032

Table 1: Mandated Reviews Overview and Frequency

Appendix A: Acronyms

CPM	Center Privacy Manager
CPO	Chief Privacy Officer
CIO	Chief Information Officer
CSPD	Cybersecurity and Privacy Division
CUI	Controlled Unclassified Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
ISO	Information System Owner
IT	Information Technology
ITS-HBK	Information Technology Security Handbook
MPII	Master Privacy Information Inventory
NASA	National Aeronautics and Space Administration
NIST	National Institute for Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OMB	Office of Management and Budget
PCAT	Privacy & CUI Assessment Tool
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RISCS	Risk Information Security Compliance System
SAOP	Senior Agency Official for Privacy
SOC	Security Operations Center
SOR	System of Records
SORN	System of Records Notice
SP	Special Publication
ViTS	Video Teleconferencing System

Appendix B: Glossary

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 M-17-12, 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, 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 policy proposals. (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].