



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 5 - Privacy Incident Response and Management

5.1 Privacy Incident Response and Management Overview

5.1.1 The Privacy Incident Response and Management chapter relates to NASA's response to incidents involving the breach of PII entrusted to NASA's custody or managed by a contractor on NASA's behalf. This chapter addresses breach response requirements within OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investment, and OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

5.1.2 The mechanism for response to a confirmed moderate or high-risk breach is a privacy Breach Response Team (BRT), which is convened within 24 hours of the incident. A Center BRT is convened when a breach of sensitive PII meets the threshold outlined in the handbooks associated with Chapter 5. Sensitive PII is a subset of PII, which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. The BRT analyzes risk of identity theft in accordance with OMB requirements and NASA policies and guidelines, prepares recommendations for remediation and notification plans, drafts breach notification letters, determines the mechanism of public notice, assists the ISO in preparing Frequently Asked Questions (FAQs), notifies and continues to provide updates to the NASA Privacy Program Manager on the status of the breach and any related breach response activities, and submits findings and recommendations to the SAOP for approval, as appropriate.

5.1.3 Non-governmental PII that is the property of the custodian, or entrusted to that person by friends or family, or a NASA contractor, grantee, etc., including corporate data used for non-governmental purposes but stored on NASA equipment is not covered by this NPR. While the limited personal use of government equipment may be permitted by NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology, NASA has no responsibility for the loss or compromise of such information.

5.1.4 NASA privacy breach response procedures are governed by ITS-HBK-1382.05, Privacy Incident Response and Management and ITS-HBK-2810.09, Incident Response and Management.

5.2 Privacy Incident Response and Management Policy

5.2.1 The SAOP shall:

- a. Establish, implement, and publish Agency PII breach response and management policies and procedures in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
- b. Review, approve, or amend BRT recommended actions and notification plans, as appropriate.
- c. Advise NASA senior management on sensitive PII breaches and remediation progress, as appropriate.
- d. Activate an Agency BRT if the situation warrants a NASA-wide activation.

- e. Advise NASA senior management when notification and action plans need to be executed at a NASA-wide level.
- f. Ensure that all NASA users receive incident reporting training as outlined in Chapter 7 of this NPR.

5.2.2 The Center CIO shall advise the BRT, as appropriate.

5.2.3 The NASA Privacy Program Manager shall:

- a. Assist the SAOP in fulfilling PII breach responsibilities.
- b. Recommend to the SAOP to activate an Agency BRT, if appropriate, and not already activated.
- c. Maintain, as appropriate, coordination and communication with the SAISO and the NASA Security Operations Center (SOC) for incident reporting, tracking, and closure of sensitive PII breaches.
- d. Provide, as necessary, overall direction to an Agency BRT for sensitive PII breaches.
- e. Provide overall breach response guidance for sensitive PII BRT activities.
- f. Update the SAOP on the status of the breach and breach response activities, as appropriate.
- g. Submit, as appropriate, BRT findings and recommendations to the NASA SAOP for approval.

5.2.4 The CPM shall:

- a. Ensure suspected loss, actual loss, and unauthorized access to PII are reported in accordance with NASA policy and procedures.
- b. Function as a core Center BRT member advising the BRT on privacy related policy, requirements, and procedures.
- c. Ensure that the steps outlined in ITS-HBK-1382.05 and ITS-HBK-2810.09 are met, as appropriate.
- d. Participate in suspected PII breach initial investigations, determinations, reporting, and response efforts.
- e. Produce reports and close out breach actions, as required.
- f. Ensure necessary followup actions on remediation efforts, in coordination with the Center CISO, are conducted to reduce risk of repeat offenses.

5.2.5 The ISO shall:

- a. Advise the BRT on the specifics of the affected information system(s) and/or information.
- b. Advise on applicable policies, processes, and impacts related to the breach.
- c. Support recommendations from the BRT.

5.2.6 The NASA user shall report any suspected or confirmed breach of any form of PII as an Information Security incident to the NASA SOC immediately upon discovery.

5.2.7 The Office of the Inspector General (OIG) shall investigate PII breaches involving suspected criminal intent in accordance with the OIG policies and coordinate with the BRT on such matters, as appropriate.

5.2.8 The Office of the General Counsel shall advise all BRTs on legal issues and review for legal sufficiency all proposed notification materials.

5.2.9 The Center Chief Counsel shall advise the Center BRT on legal issues and review for legal sufficiency proposed notification materials, as appropriate.

5.2.10 The Center Public Affairs Office may:

- a. Advise on, and review, proposed notification materials and approaches.
- b. Generate releases and other public notifications as requested.

5.2.11 The CO/COTR, in situations where the breach involves information maintained on NASA's behalf by or on contractors, shall serve as the interface between government and contracting parties. 5.2.12 The Center Human Resources Employee Relations Specialist may:

- a. Designate an Human Resources staff member to serve as a member of the BRT. The designated staff member will participate in gathering and documenting information and evidence about the role of any civil servant employee in the breach.
- b. Advise the civil servant's supervisor(s) on appropriate corrective action, which may include formal or informal disciplinary action.

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