Information Technology Requirement

Personally Identifiable Information (PII) Breach Response Policy

NITR-1382-1
Version Date: 20071213
Effective Date: 20071221
Expiration Date: 20091221
Responsible Office: Office of the Chief Information Officer

Revision Record

ITEM NO.	REVISION	DESCRIPTION	DATE
1	V.1.0	Initial	Dec 13, 2007

Personally Identifiable Information (PII) Breach Response Policy

Purpose

This NASA Information Technology Requirement (NITR) establishes Agency procedural requirements for properly responding to a suspected or confirmed breach of personally identifiable information (PII).

Scope

The requirements identified in this document apply when there is an identification of a potential breach of personally identifiable information (PII) as defined in NPR 1382.1. For the purposes of this policy, the term "breach" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users or for other-than-authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Note that in the case of a suspected PII breach which occurs through the loss of a government computer, PDA or thumb drive, the PII addressed by this policy is limited to PII that is entrusted to NASA's custody or managed by a contractor on NASA's behalf. PII that is the personal property of the equipment custodian, or entrusted to that person by friends or family is not covered by this policy, e.g., a personal address book or family financial information. This limited personal use of government equipment may be permitted by NPD 2540.1F, Personal Use of Government Office Equipment Including Information Technology, but NASA has no responsibility for the loss or compromise of such information.

The policies and processes for the handling of PII breach incidents are herein defined at the Agency level. These policies and processes are executed at the Center level unless the magnitude of the incident warrants otherwise.

Applicability

This policy applies to NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. It also applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, and to parties to agreements, to the extent that they maintain PII on NASA's behalf.

Authority

a. NASA Policy Directive (NPD) 1382.17, NASA Privacy Policy.

b. NASA Procedural Requirement (NPR) 2810.1, NASA Information Technology Security Requirements

c. Clinger Cohen Act of 1996, 40 U.S.C. § 1401.

d. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3535.

e. Privacy Act of 1974, 5 U.S.C. § 552a.

f. OMB Memorandum dated September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification

g. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

Requirements

1. Employees and contractors across the Agency shall immediately report any suspected breach of PII as an IT Security incident through the procedure defined in NASA's ITS-SOP-015, Procedure for IT Security Incident Classification and Reporting located in the NASA Online Directives Information System (NODIS) at http://nodis-dms.gsfc.nasa.gov/restricted_directives/SOP_restricted/SOP_list.cfm., with the Information Technology Security Manager (ITSM) notifying NASA Incident Response Center (NASIRC), and NASIRC notifying the United States Computer Emergency Response Team (US-CERT) within one hour of receiving the report.

2. Each Center Chief Information Officer (CIO) shall establish and lead a "Breach Response Team" (BRT) in the event of a suspected PII breach. This team will report its findings and recommendations to the NASA Senior Agency Privacy Official (SAPO).

a. The BRT must be comprised of the following required members:

- Center CIO
- Center Information Assurance Officer
- Center Privacy Act Manager
- Center ITSM
- The functional lead, system owner and the data owner of the affected system and data

Note that individuals who are the functional leads, the system owners and the data owners of the affected systems and data may vary from incident to incident

The ITSM will notify the system owner of the breach as part of the incident investigation process. As BRT lead, the Center CIO will advise the functional lead, system owner and data owner of when the BRT will convene.

b. The BRT membership may also include one or more of the following additional members from the following offices, as the individual situation warrants:

- Office of the Inspector General
- Center Chief Counsel or designee
- Center Public Affairs Office/Strategic Communications Office
- Contracting Officer/Contracting Officer's Technical Representative
- Center Human Resources Employee Relations
- Other Subject Matter Experts as needed

The Center Chief Counsel or designee will be notified of all breaches and be involved in the BRT unless at their discretion they determine their presence unnecessary.

3. The BRT will perform the following procedures which are further described in ITS-SOP-0044, Procedures for Responding to a Breach of PII:

a. Investigate the incident
b. Evaluate and document the risk of harm posed by the incident
c. Identify and execute the appropriate steps to be taken to contain and mitigate harm at the system and data level
d. Identify and execute system and policy improvements to be made to prevent future breaches
e. Identify protective measures NASA will take on behalf of affected individuals
f. Identify protection recommendations that affected individuals should take on their own behalf
g. Determine what notification steps should be taken to inform affected individuals
h. Communicate findings and recommendations to the SAPO in a prompt manner

4. With concurrence of the SAPO and Agency Management (where appropriate based on the size and scope of the incident), recommended actions shall be carried out at the approved level. Actions and notifications occur from the local or agency level BRT lead unless another source of notification is determined by the SAPO to be more appropriate (e.g., in the case where it is deemed prudent for the notification to come from Headquarters or the Administrator).

Responsibilities

BRT: Performs the investigation of a breach and prepares recommendation of remediation actions and notification plan.

Center CIO: Leads the BRT. Responsible for directing actions involving IT infrastructure. Advises the functional lead and system/data owner of affected systems about the meeting of the BRT.

Center ITSM: Investigates the incident according to NASA NITRs, IT Security Standard Operating Procedures and processes. Maintains record of all technical, remediation, risk assessment and notification actions taken. Advises the BRT on technical aspects of the breach and exposure.

Center Information Assurance Officer: Assesses the appropriateness of policies and procedures to protect PII in the context of the breach. Recommends changes and improvements to policies and procedures as appropriate.

Center Privacy Act Manager: Advises the BRT on privacy related matters.

Functional leads and system/data owners of affected systems: Advises the BRT on the specifics of the affected systems and data. Advises on applicable policies, processes and impacts related to the breach context. Performs remediation as directed by BRT.

Office of the Inspector General: Investigates breaches involving suspected criminal intent in accordance with the Agency IT Security Incident Response process. Advises the BRT on such matters.

Center Chief Counsel: Advises the BRT on legal issues and reviews for legal sufficiency proposed notification materials.

Center Public Affairs Office/Strategic Communications Office: Advises on and reviews proposed notification materials and approaches.

Contracting Officer (CO)/Contracting Officer's Technical Representative (COTR): In situations where the breached information was in the custody of a NASA contractor and being maintained on NASA's behalf, or where the information breached was information in NASA's custody about NASA contractors, the CO/COTR serve as the interface to the contractor and the communication conduit.

Center Human Resources Employee Relations: Advises in situations where disciplinary action may be taken against a civil servant.

Other Subject Matter Experts: Advise on specific topics relevant to processing the breach

SAPO: Responsible for approving recommended actions and notification plans. Expands or escalates BRT activities as necessary. Advises Agency Management on situation and progress.

Agency Senior Management: Execute notification and actions plans when situation is appropriate for action to be taken at that level.

References

a. NPR 1382.1, NASA Privacy Procedural Requirements.

b. NPR 1600.1, NASA Security Program Procedural Requirements.

c. NPD 2540.1F, Personal Use of Government Office Equipment Including Information Technology

d. ITS-SOP-015, Procedure for IT Security Incident Classification and Reporting.

e. ITS-SOP-0044, Procedures for Responding to a Breach of PII

f. OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources.

g. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information

h. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments.

Approval

Jonathan Q. Pettus

Jonathan Q. Pettus
NASA Chief Information Officer

12-21-07
Date