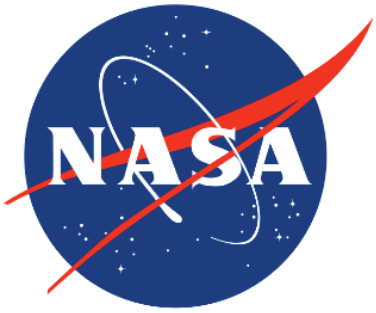

Information Technology Security Handbook

Privacy Incident Response and Management: Breach Response Team Checklist

July 2022

Version 1.4.0

OFFICE OF THE CHIEF INFORMATION OFFICER

CYBERSECURITY AND PRIVACY DIVISION

Document Properties

Maintained by: OCIO CSPD Team

Filename: ITS-HBK-1382.05-01 Privacy Incident Response and Management: Breach Response Team Checklist

Related Policies:

- NASA Policy Directive (NPD) 1382.17, *NASA Privacy Policy*
- NPD 2540.1, Acceptable Use of Government Office Property Including Information Technology
- NASA Procedural Requirements (NPR) 1382.1, *NASA Privacy Procedural Requirements*
- ITS-HBK-2810.09-02A, Incident Response and Management: NASA Information Security Incident Management

Supersedes:

Version 1.3

Table 1: Revision History

Version	Date	Section	Description	Changes by
1.0	09/25/2012	Throughout	Initial Version.	OCIO CSPD Team
1.1	08/31/2015	Throughout	Associate CIO approved and signed handbook.	OCIO CSPD Team
1.2	06/28/2017	Throughout	Updated to align with OMB M-17-12 requirements.	OCIO CSPD Team
1.3	10/11/2018	Throughout	Annual update mandated by OMB M-17-12.	OCIO CSPD Team
1.4	07/14/2022	Throughout	Minor updates, reviewed by privacy personnel at the center and agency level.	OCIO CSPD Team

Table of Contents

1. INTRODUCTION 1
2. PURPOSE 1
2.1 Scope 1
3. POINT OF CONTACT(S) 2
4. APPLICABILITY 2
5. APPLICABLE DOCUMENTS 2
6. PRIVACY INCIDENT RESPONSE AND MANAGEMENT PROCESS 3
7. BRT Checklist 3
Appendix A: Acronyms 14
Appendix B: Glossary 15
Appendix C: Sensitive Personally Identifiable Information (PII) Breach RESPONSE Plan TEMPLATE 16
1. Summary 17
2. Scope 17
3. Assumptions 17
4. Roles and Responsibilities 17
5. Sensitive PII Definition 18
6. Notification and Activation Phase 18
6.1. Notification 18
6.2 Activation 18
7. Recovery Phase 19
8. Deactivation 19

Figure 1 Informal BRT (Small Scale Breach) 18
Figure 2 BRT Diagram 19

This page intentionally left blank.

Distribution:

CSET

[redacted]

Associate Chief Information Officer for
Cybersecurity & Privacy

1. INTRODUCTION

National Aeronautics and Space Administration (NASA) requirements for the protection of NASA information and information systems derive from the 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 and in the selection and implementation of information security controls consistent with authorities listed in Sec. 5 below.

2. PURPOSE

According to NPR 1382.1, NASA Privacy Procedural Requirements, this handbook governs NASA's privacy breach response procedures. This handbook provides privacy Breach Response Teams (BRTs) and Agency/Center Privacy Managers (A/CPMs) with the tools and resources needed to quickly initiate a BRT and follow the required steps and processes (outlined within the BRT checklist).

This handbook supports the implementation of requirements in NPD 1382.17, NASA Privacy Policy and NPR 1382.1. 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 organization-defined values are integrated into the control requirements within the Risk Information Security Compliance System (RISCS) system.

This handbook outlines the NASA Privacy Breach Response Team (BRT) checklist for implementing the privacy breach response requirements set out in Appendix I of ITS-HBK-2810.09-02, *Incident Response and Management: NASA Information Security Incident Management*. A well-prepared and trained BRT is key to meeting the communication and notification requirements outlined within NASA policy related to a breach of sensitive personally identifiable information (PII). The BRT checklist serves as an aid to Centers in all aspects of the privacy BRT process from initiation through closeout.

A/CPMs are responsible for tailoring the checklist to include Center specific procedures to a privacy breach; thereby, ensuring that the Center has the resources it needs should a privacy breach occur. In addition, the handbook includes a sample Sensitive PII Breach Response Plan.

2.1 Scope

This handbook supplements Chapter 5 of NPR 1382.1. Compliance with this Handbook and/or Chapter is mandatory. Non-compliance or any unauthorized or improper use of NASA IT may result in the suspension or revocation of access to NASA IT, disciplinary action, as well as civil and criminal penalties.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the policy guidance or procedural requirements outlined 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 A/CPM, to review and validate for the record.

In this handbook, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

In this handbook, all document citations are assumed to be the latest version unless otherwise noted.

3. POINT OF CONTACT(S)

Stayce Hoult, NASA Chief Privacy Officer (CPO):

- stayce.d.hoult@nasa.gov

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 and directed to the attention of the point of contact for this particular Handbook to address and resolve.

4. APPLICABILITY

This handbook applies to NASA Headquarters and NASA Centers. NASA Centers include Component Facilities, 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.

5. APPLICABLE DOCUMENTS

Federal Laws and Regulations

- Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896

Office of Management and Budget (OMB)

- Office of Management and Budget (OMB) Memorandum M-07-04, Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)
- OMB M-16-14 Category Management Policy 16-2, Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response
- OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information

National Standards of Standards and Technology (NIST)

- NIST 800-60 Volumes 1 and 2, Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST Special Publication (SP) 800-53 Rev.5, Recommended Security Controls for Federal Information Systems and Organizations)
- Risk Management Framework (NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

National Aeronautics and Space Administration (NASA)

- NPD 2810.1, *NASA Information Security Policy*
- NPR 2810.1, *Security of Information and Information Systems*

- NASA Policy Directive (NPD) 1382.17, *NASA Privacy Policy*
- NASA Procedural Requirement (NPR) 1382.1, *NASA Privacy Procedural Requirements*
- ITS-HBK-2810.09-02A, *Incident Response and Management, NASA Information Security Incident Management*

6. PRIVACY INCIDENT RESPONSE AND MANAGEMENT PROCESS

The steps regarding the Privacy Incident Response and Management Process are outlined in ITS-HBK-2810.09-02A. Those steps should be followed when responding to a breach of sensitive PII.

7. BRT CHECKLIST

The following checklist provides basic step-by-step tasks that BRTs shall follow in the event of a sensitive PII breach. The areas are listed sequentially. Areas where Center specific tasks may govern are highlighted throughout the checklist. Each A/CPM shall tailor those highlighted portions of this checklist to align with the Center local processes within 90 days of the validation of this handbook, provide each member of the BRT with a copy of the checklist, and save their updated checklist to the Privacy SharePoint site.

Tasks	Supplemental Guidance
☐ 1. The NASA Security Operations Center (SOC) is notified of suspected or confirmed breach of PII immediately upon discovery.	*No BRT action is required.* It occurs prior to the BRT convening. The NASA user is obligated to immediately notify the NASA SOC of a suspected or confirmed breach of PII.
☐ 2. The SOC makes a report on the suspected or confirmed breach of PII in the Incident Management System (IMS).	*No BRT action is required.* This occurs prior to the BRT convening. The SOC report will include: • Date and time of discovery of suspected or confirmed breach of PII. • Clear and detailed information on the type of PII suspected or confirmed to have been involved in the breach. Note: The SOC ticket number shall be included in all BRT Report submissions to the NASA Chief Privacy Officer (CPO), whether reporting on preliminary BRT activities or submitting the final report upon event closure. SOC reports shall be updated throughout the BRT process as updates occur, and the SOC ticket should not be closed until the full completion of all activities. This action may be undertaken by the Center Chief Information Security Officer (CISO), Incident Response Manager (IRM), or an Incident Response team member when NASA users do not report discovery through the SOC as required.

☐ 3. United States Computer Emergency Readiness Team (US-CERT) Notification. ☐ a. The NASA SOC notifies US-CERT of the suspected or confirmed breach of PII within one hour.	*No BRT action is required.* This occurs prior to the BRT convening. *No BRT action is required.* This occurs prior to the BRT convening. The NASA SOC is mandated to report within one hour per NASA procedure, under the *OMB M-18-02* and *US-CERT Federal Incident Notification Guidelines*[1].
☐ 4. The SOC notifies the IRM and A/CPM of the suspected or confirmed breach of PII. ☐ a. The A/CPM follows up with the SOC to verify that the one-hour requirement for reporting to US-CERT has been met.	*No BRT action is required.* This occurs prior to the BRT convening. This is generally an automatic process initiated when the SOC report is assigned. **Note:** The IRM for a PII breach is not typically the A/CPM. This sub-step can occur in sequence or after a BRT has been convened at the discretion of the A/CPM. However, this shall occur within the first 48 hours after a privacy breach. The A/CPM should document that this task was completed on the preliminary BRT Report. If the one-hour reporting requirement has not been met, the A/CPM shall record justification or explanation for the failure to meet the requirement and will immediately notify the NASA CPO.
☐ 5. The IRM contacts and coordinates with the A/CPM.	This constitutes the initial convening of the preliminary BRT. This occurs prior to the BRT officially convening. The order of this notification may vary based on Center processes.
☐ 6. The A/CPM initiates a BRT Report.	The A/CPM officially initiates a BRT Report upon the affirmation that a BRT is convening due to the suspected or confirmed breach of PII. The BRT report will be updated regularly throughout the BRT cycle and will be used to apprise the CPO as updates occur. Upon full closure of privacy BRT activities, the completed BRT Report will be submitted to the NASA CPO via encrypted e-mail directly.
STEP 1: INITIAL INVESTIGATION & DETERMINATION	

[1] US-CERT Federal Incident Notification Guidelines | CISA

☐ 7. The IRM and A/CPM perform a basic assessment to determine if the incident is a confirmed breach of PII and to qualify the PII as either sensitive or non-sensitive.	This is a coordinated decision between the IRM and the A/CPM. If there is doubt as to whether the information is sensitive PII, the A/CPM may contact the NASA CPO in the Chief Information Officer's Office (OCIO). Sensitive PII is a combination of PII elements, which, if lost, compromised, or disclosed without authorization, could be used to inflict substantial harm, embarrassment, inconvenience, or unfairness to an individual. NASA makes a distinction between sensitive and non-sensitive PII. To help determine the nature of the data elements that have potentially been breached, refer to the relevant Privacy Threshold Analysis (IPTA), Privacy Impact Assessment (PIA), or System of Records Notice (SORN) in the RISCS Privacy Solution in RISCS.
☐ 8. The IRM and A/CPM determine if other responsible parties should be included in the formal BRT. IRM/A/CPM should determine how large the team must be to resolve the incident and who will be its core members. Asterix indicates typical BRT core.	The IRM and A/CPM work together to evaluate initial reports, make determinations regarding sensitivity, recommend immediate steps for remediation, identify next steps, and formulate recommendations to be delivered to the BRT Lead (see diagram below). This activity constitutes an informal BRT. Circumstances may require the convening of a formal BRT. Members of the formal BRT might include: • Center Chief Information Officer (CIO) - Most breaches require CIO notification at the least, if not Center CIO involvement in the BRT itself • *Center CISO • *CPO • OCIO staff (at the very least, the BRT Liaison acts as the connection to the OCIO.) • Inspector General (IG) is involved where there is a suspected criminal intent. • Center Chief Counsel - Specifically, for review of any breach notification determinations and materials. • Center Public Affairs, News Chief - specifically, for review of any breach notification materials related to media outlets.

	• Contracting Officer (CO)/CO Representative (COR) when a contractor is involved in the breach. • Center Human Resources Employee Relations Representative • Subject Matter Experts (SMEs) Note: If a privacy breach impacts multiple Centers, this list shall be expanded appropriately.
☐ 9. A BRT Lead is established. The BRT Lead gathers all applicable documents needed for the response to the privacy breach and ensures that all BRT members are provided with a copy of the applicable documents.	The BRT Lead will act as the facilitator/coordinator for the BRT effort. The BRT Lead will ensure that all BRT members have applicable policies and procedures to respond to the PII Breach. Additionally, the BRT Lead will ensure that all appropriate and necessary documentation is kept throughout the response period. Finally, the BRT Lead is the individual who has decision authority for recommendations from the BRT. The BRT lead may be the Center CIO or their designee.
☐ 10. The IRM and A/CPM formulate initial recommendations to present to the BRT Lead.	Recommendations from the initial assessment should be consolidated and presented to the BRT Lead.
☐ 11. The A/CPM notifies the NASA CPO of the privacy breach and the activation of the BRT.	The A/CPM is required to keep the NASA CPO abreast of all privacy breach activities. The BRT Report is one of the mechanisms used by the A/CPM to keep the CPO up to date.
☐ 12. The A/CPM confirms with the SOC that the one-hour requirement for reporting to US- CERT has been met and ensures the Privacy BRT Report is updated with specifics.	This step may have already occurred in 4.a.; the order in which this occurs is at the discretion of the A/CPM. However, this shall occur within the first 48 hours after a privacy breach. If the one-hour reporting requirement has not been met, the CAM shall record justification or explanation for the failure to meet the requirement and will immediately notify the NASA CPO.
STEP 2: INITIAL MITIGATION	
☐ 13. Work the steps outlined in *ITS-HBK- 2810.09-02* to define and implement necessary actions to minimize or secure the potential growth of the incident.	Determine if the technology involved needs to be confiscated. The BRT may need to work with Office of Protective Services (OPS) to determine if this action is appropriate.

☐ 14. The BRT initially assesses degree of potential data compromise.	Each privacy breach is unique and should be reviewed and mitigated in accordance with the circumstances of the privacy breach.
STEP 3: BREACH RISK ASSESSMENT	
☐ 16. The BRT establishes a plan for necessary interviews to complete this step.	Depending on the nature of the privacy breach, interviews may be conducted by members of the BRT. Each breach is different and requires an analysis of which individuals or groups are appropriate to conduct the necessary interviews. The use of a Risk Assessment Matrix that scores each factor may be helpful to determine the overall risk of harm. The BRT Core Team should perform the risk assessment since only these individuals will know the most sensitive details of the breach.
Factor 1 – Nature and Sensitivity of the Data Elements Breached	
☐ 17. The IRT and A/CPM identify the data elements potentially breached and documents them in the BRT Report.	The nature and sensitivity of the data elements breached is key to determining the overall risk associated with the privacy breach – it provides context for the decisions the BRT will make regarding the categorization of the privacy breach [Low, Medium, High] and the actions required to take as a result.
Factor 2 – Number of Individuals Affected	
☐ 18. The BRT Core identifies the number of individuals affected and documents it in the BRT Report.	Remember that a privacy breach is a breach regardless of the number of individuals impacted. **Note:** If the number is unknown or growing, individuals are identified, and notification is deemed appropriate (defined in Step 4(b) of this handbook), start the notification process.
Factor 3 – Likelihood the Information is Accessible and Usable	

☐ 19. The BRT Core determines the likelihood that the information is accessible by unauthorized individuals and documents the findings in the BRT Report.	The fact that the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. Factors that the BRT should consider when determining whether information is accessible are: • Security safeguards employed (i.e., whether the information was encrypted or rendered unusable by other means.) • Whether the format and media of the PII may make it resource-intensive to use. For example, a flash drive is more likely to be used than a magnetic tape cartridge used for backing up servers. **Note:** If the information is neither accessible, nor usable, the risk categorization [Low, Medium, High] is likely Low.
☐ 20. The BRT Core determines the likelihood that the information is usable by unauthorized individuals and documents the findings in the BRT Report.	Specifically, whether the individual(s) that have the information know the value of the information. **Note:** If the information is neither accessible, nor usable, the risk categorization [Low, Medium, High] is likely Low.
Factor 4 – Likelihood the Breach May Lead to Harm	
☐ 21. The BRT Core determines the nature of the potential harm that may result from the privacy breach and documents the findings in the BRT Report. The nature and sensitivity of the compromised information depends on the specific data elements compromised, but also on other factors such as: • Context of the information • Private information • Relevance to vulnerable populations • Long-term or permanent applicability of the information	Such harm may include the effect of a breach of confidentiality, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem. Refer to *OMB Memorandum M-17-12* Section 7E for guidance on how to assess the risk of harm and/or embarrassment. The application of human judgment is critical in weighing the factors that may contribute to the nature of potential harm from a breach. In addition, the Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to

	any individual on whom information is maintained" (*5 U.S.C. 552a(e)(10)*).
☐ 22. The BRT Core determines the likelihood that harm may occur from the privacy breach and documents the findings in the BRT Report.	This decision is based on the types of data involved in the incident. In considering whether the loss of information could result in identity theft or fraud, additional consultation may be obtained in guidance from the President's Identity Theft Task Force at http://www.idtheft.gov.[2]
Factor 5 – Ability of the Agency to Mitigate the Risk of Harm	
☐ 23. The BRT Core determines the ability of NASA to mitigate the risk of harm and documents the findings in the BRT Report.	This relates to NASA identifying what is required to mitigate further compromise or minimize the associated harm.
☐ 24. The BRT Core implements appropriate mitigation actions that have not already been taken during *Step 2 Initial Mitigation*.	This is done to minimize the associate harm.
Outcome – Risk Determination	
☐ 25. The BRT Core makes a breach risk determination [Low/Medium/High].	The BRT will look at the overall result of the risk assessment: Likelihood x Impact = Risk. Determination is made as to what actions are appropriate to take in ITS-HBK-2810.09-02, Appendix G *Step 4(a)* and *Step 4(b)*.

[2] This decision is based on many factors. All aspects of incidents must be assessed to make a final decision on likelihood that harm may occur. Aspects of what should be considered include: the specific data elements involved, the level of sensitivity for these elements of information as they stand alone, and as they are combined. Considerations that should be applied include whether the loss of information could result in identity theft, fraud, harm, or embarrassment.

☐ 26. The BRT Lead contacts the CPO to discuss the initial privacy breach risk assessment determination [Low/Medium/High].	The BRT Lead and/or the A/CPM may contact the CPO.
STEP 4(A): EXTERNAL MITIGATION RECOMMENDATION	
☐ 27. The BRT determines which external mitigation actions will be recommended or provided by NASA. ☐ a. The BRT determines if the risk necessitates commercial credit monitoring or identity monitoring services be provided to the individuals impacted by the privacy breach. In accordance with OMB Memorandum M-16-14, credit or identity monitoring services must be acquired through GSA BPAs. The organizational unit (division, department, or Center) responsible for the breach is also responsible for procuring and funding credit monitoring services. ☐ i. If credit or identity monitoring services are acquired outside of the GSA BPAs, the NASA CPO must notify GSA and OMB in accordance with OMB Memorandum M-07-04 ☐ ii. [Include Center process for obtaining credit monitoring] ☐ iii. Ensure that contracted service providers' notifications and alerts to affected individuals comply with Section 508 of the Rehabilitation Act of 1973 (through contract language).	Specific information on the potential NASA and individual actions that can be taken is found in *ITS-HBK-2810.09.02NASA Information Security Incident Management*, *Appendix G Step 4(a)*. Draft notification letter language informing affected individuals of steps they should take following a privacy breach is addressed in *Step 4(b)*. Commercial credit or identity monitoring is not always required. These services are possible provisions a BRT can decide to use. If it is decided that a provision is in the best interest of those who have had their information compromised and the government, the Government Services Administration (GSA) has an established Blanket Purchase Agreement (BPA) in place, under which a minimum of 3 providers are listed to facilitate procurement of commercial credit or identify monitoring services. The responsibility for procurement and funding of these services depends on the details surrounding the privacy breach. The BRT will review and make the appropriate determinations. Typically, if circumstances demand other arrangements, the BRT Lead should work with the Center CIO to fully investigate and resolve any questions in support of all possibly expediency. If the Center CIO is not able to reach an agreement with the breaching organization, the Center CIO should reach out to the Senior Agency Official for Privacy (SAOP) and the NASA CPO.

☐ 28. The BRT Liaison updates the CPO on the external mitigation actions that the BRT has determined is appropriate for the privacy breach.	[Include additional Center details related to obtaining credit monitoring]
STEP 5: Notifications and other Communications	
☐ 29. The BRT develops a plan to notify individuals impacted by the privacy breach and documents the findings in the BRT Report. ☐ a. Element 1: The BRT determines whether Breach Notification is required based on the privacy breach risk assessment outcome from Step 3. ☐ i. If the BRT determines that notification is not required, the BRT Lead immediately informs the CPO of the decision. (Skip to 30). The OCIO can override the BRT's decision not to provide the notification. ☐ b. Element 2: The BRT determines when notification will be provided and establishes a target date for release. ☐ i. If notification is going to be delayed, the BRT Lead shall coordinate with the CPO to obtain approval to delay from the SAOP or their designee. ☐ c. Element 3: The BRT determines the appropriate source of privacy breach notification and who at NASA should be listed on the notification letter for recipients to contact. ☐ d. Element 2: The BRT determines when notification will be provided and establishes a target date for release. ☐ i. If notification will be delayed, the BRT Lead shall coordinate with the CPO to obtain approval to delay from the SAOP or their designee. ☐ 1. The NASA CPO works with the NASA Office of General Counsel (OGC) to review and recommend revisions to the notification as appropriate. ☐ ii. The NASA CPO concurs with the notification and provides any applicable	[Notice shall be provided without unreasonable delay, consistent with law enforcement measures and Incident Response measures. Note that if IPS or credit monitoring services will be provided (which could take some time to procure) to give a timely notice to those affected, two notifications may need to be sent out. An initial notification will mention that a second notification is coming that will contain enrollment instructions for the IPS or credit monitoring services. If circumstances dictate that notifications could increase the risk of harm and it is more prudent not to provide notification or delay notification, safeguards should be put in place and delays justified in writing for submission and determination/approval by the SAOP. Notice shall be provided without unreasonable delay, consistent with law enforcement measures and Incident Response Team measures. Only the SAOP or their designee may decide that delay is permissible. The source of privacy breach notification is dependent on the breach itself. The source should be at the level appropriate to the magnitude and scope of the privacy breach. If a privacy breach has occurred at several Centers, it may be appropriate for the SAOP, NASA CIO, other NASA senior official, or the NASA Administrator to sign the notification letters.

updates to the letter to the BRT Lead. e. Element 5: The BRT determines the means of providing privacy breach notification. f. Element 6: The BRT determines who should receive the privacy breach notification.	The OGC, SAOP, and NASA CPO have the authority to revise the content and provide revised language for notification letters. The potential means of notification are outlined in ITS-HBK-2810.09-02, Appendix G. The groups that receive the notification may vary depending on the privacy breach. It may range from the individuals affected, to legal guardians of those individuals, to groups of individuals, to the media. Note: If the media is to receive the notification, the News Chief or external communications at the Center shall be engaged.
☐ 30. The BRT briefs Center senior leadership on the BRT recommendations and actions, as appropriate.	Based on the nature of the privacy breach, there may be several Center senior leadership briefings throughout the BRT process.
☐ 31. If notification is appropriate, the source of the notification identified in Element 3 signs the notification.	Notification letters can be sent as attachments to the e-mail if circumstances support it, to expedite the process, if notification is emailed, careful consideration should be given to determine whether notifications are encrypted. Second notifications containing IPS or credit monitoring services are usually sent via the U.S. postal service from the vendor with a gif of the NASA officials signature and a NASA POC for affected individuals to contact. If notifications are physical letters, they should be on NASA letterhead and in color.
☐ 32. Prior to any notification being sent out to the individuals impacted, the BRT Lead shall reach out to the Help Desk and the NASA SOC to provide them with a copy of the notification and the appropriate Center contact information for those who have questions.	This step is critical as many individuals may find the notification suspect and reach out to the help desk or the SOC for additional information or validation. Care should be given when drafting and sending letters (especially if emailing them) to ensure they do not appear as junk mail or spam.

☐ 33. The privacy breach notification is sent to the individuals identified in Element 6.	The BRT Report is updated, and the CPO is notified that this step was completed. The Center Privacy BRT Chair identifies which office is responsible for sending the breach notification letter.
☐ 34. The BRT Lead assesses the privacy breach and the privacy breach response. The Lead thoroughly documents any lessons learned and corrective actions taken, and any other relevant details in the BRT Report.	The A/CPM has access to the BRT Report. Lessons learned, corrective actions, and other relevant details along with all BRT costs for the specific privacy breach activity - including remedial actions, provided services, and man-hours for all of those who participated in the BRT activities - shall be documented fully in the appropriate sections of the BRT report. The working hours of the IRM and IRT should not be included in the spread sheet matrix since they report directly to the SOC.
☐ 35. The BRT Lead sends a signed copy of the notification and all supporting information provided to those affected (including information relative to credit services or identify monitoring) to the CPO.	[Include additional Center details related to obtaining credit monitoring] Notification steps 29-35 may need to be repeated for a second notification if an initial notification was sent.
☐ 36. The BRT Lead supports the finalization of the BRT Report and submits it to the CPO as the official record of the privacy breach upon closure of the event in the IMS (but not as part of IMS closure or IRM reporting).	Based on the nature of the privacy breach, there may be several Center senior leadership briefings throughout the BRT process. A/CPM concurrence of the report is required prior to the finalization of the BRT Report. The BRT Report is sent to the CPO by the A/CPM and shall include a full accounting of privacy breach costs (person-hours, remediation, etc.). The privacy BRT Report is a Privacy program-specific requirement with responsibility solely with the A/CPM for its creation, update, validation, and submission. The privacy BRT Report has no effect, delay, or contingency on any other IRM reporting requirements. The A/CPM works directly with the CPO to negotiate any extensions or issues with this report. The BRT Report should be posted to the appropriate repository.

APPENDIX A: ACRONYMS

BRT	Breach Response Team
BPA	Blanket Purchase Agreement
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Contracting Officer
COR	Contracting Officer Representative
A/CPM	Agency/Center Privacy Manager
CPO	Chief Privacy Officer
CSPD	Cybersecurity and Privacy Division
CUI	Controlled Unclassified Information
FIPS	Federal Information Processing Standards
GSA	Government Services Administration
HBK	Handbook
IG	Inspector General
IMS	Incident Management System
IPTA	Initial Privacy Threshold Analysis
IRM	Incident Response Manager
ISO	Information System Owner
ITS	Information Technology Security
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
OGC	Office of General Counsel
OMB	Office of Management and Budget
OPS	Office of Protective Services
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
RISCS	Risk Information Security Compliance System
SAOP	Senior Agency Official for Privacy
SME	Subject Matter Expert
SOC	Security Operations Center
SORN	System of Records Notice
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team
U.S.C.	United States Code

APPENDIX B: GLOSSARY

Non-Sensitive PII	Non-Sensitive PII is information that is available in public sources; the disclosure of which cannot reasonably be expected to result in personal harm.
Sensitive Personally Identifiable Information (PII)	Sensitive PII is a subset of PII that, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. a. Examples of stand-alone PII include Social Security Numbers (SSN), driver's license or state identification number; Alien Registration Numbers; financial account number; and biometric identifiers such as fingerprint, voiceprint, or iris scan. b. Additional examples of SPII include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements: 1. Truncated SSN (such as last four digits) 2. Date of birth (month, day, and year) 3. Citizenship or immigration status 4. Ethnic or religious affiliation 5. Sexual orientation 6. Criminal history 7. Medical information 8. System authentication information such as mother's maiden name, account passwords, or personal identification numbers. c. Other PII may be "sensitive" depending on its context, such in as a list of employees and their performance rating(s) or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive. NOTE: Although the Universal Uniform Personal Identification Code (UUPIC) is a unique identifying number, NASA does not consider it as sensitive PII.

APPENDIX C: SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH RESPONSE PLAN TEMPLATE

Sensitive PII Breach Response Plan[3]

[CENTER]

Version:

Date:

[3] This appendix is meant to be cut and pasted into a Word document to serve as your breach response plan. It has its own two appendices to record your change history and call-down plan.

1. Summary

- The [CENTER] Breach Response Team (BRT), Privacy Information Breach Plan establishes the Center procedures for responding to a breach of sensitive Personally Identifiable Information (PII). The following four steps of a privacy breach response and privacy breach close out have been established for this plan to maximize the effectiveness of sensitive PII breach response from privacy breach identification:
- Step 1: Initial Investigation and Determination
- Step 2: Initial Mitigation
- Step 3: Breach Risk Assessment
- Step 4(a): External Mitigation Recommendations
- Step 4(b) Breach Notification Recommendation
- The following objectives have been established to maximize the effectiveness of sensitive PII breach response from privacy breach identification:
- To identify the activities, resources, and procedures needed to carry out the Sensitive PII Breach Plan.
- To assign responsibilities to designated personnel and guide a sensitive PII breach.
- To ensure coordination with other staff who will participate in the BRT.
- To ensure proper communication between the Center and the OCIO.

2. Scope

This plan applies to any sensitive PII breach at [CENTER].

3. Assumptions

The following assumptions were used when developing this Sensitive PII Breach plan:

Key Center personnel have been identified and trained in their privacy breach response roles and can activate the [CENTER] BRT.

4. Roles and Responsibilities

The responsibilities outlined below are pulled from ITS-HBK-2810.09-02, Incident Management and Response: NASA Information Security Incident Management and from [CENTER] requirements for the BRT and the BRT members.

BRT Lead:

Makes the final BRT recommendation decision regarding all BRT steps.

Facilitates the BRT.

Ensures that all BRT related documentation is maintained throughout the incident and provided to the NASA Chief Privacy Officer (CPO) at the conclusion of BRT activities.

BRT Agency Liaison

Acts as the liaison between the BRT and the NASA Chief Privacy Officer to ensure that the Senior Agency Official for Privacy (SAOP) is kept up to date on privacy breach activities.

Agency/Center Privacy Manager (A/CPM)

Acts as an SME for sensitive PII Breach Response on the BRT as a Core Team member.

Determines if sensitive PII is involved.

5. Sensitive PII Definition

Sensitive PII is a combination of PII elements, which, if lost, compromised, or disclosed without authorization, could be used to inflict substantial harm, embarrassment, inconvenience, or unfairness to an individual.

6. Notification and Activation Phase

During this phase the initial actions to communicate the privacy breach to the BRT members and to the Agency take place.

6.1. Notification

The Notification (i.e., communication) sequence is listed below:

1. SOC notifies IRM and A/CPM of a suspected breach of sensitive PII.
    a. IRM and A/CPM joint together to form an informal BRT, as appropriate.
2. A/CPM notifies NASA Agency (NASA Chief Privacy Officer) of the confirmed breach of sensitive PII.
    a. If a formal BRT is not convened, the A/CPM updates the NASA Chief Privacy Officer on the status of the privacy breach throughout the privacy breach process.
3. IRM and A/CPM contact core BRT members to form a formal BRT, as appropriate.
4. BRT Lead contacts additional BRT members as is appropriate to the nature of the privacy breach.
5. BRT Agency Liaison communicates with the NASA Chief Privacy Officer regarding the privacy breach.

6.2 Activation

The Sensitive PII Breach Plan is to be activated once a sensitive PII breach is confirmed. The following two charts outline the BRT based on the size and the nature of the sensitive PII Breach.

Small scale sensitive PII Breach – the BRT is as follows:

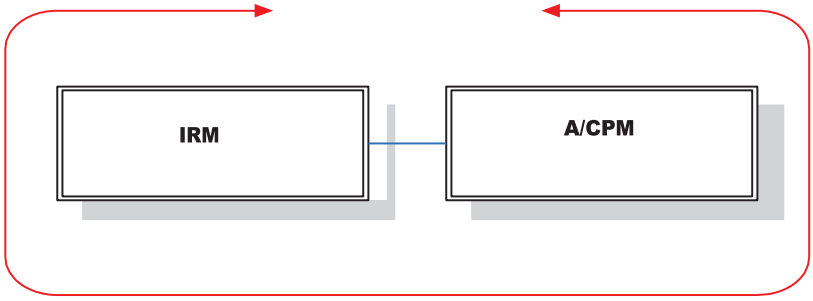

Figure 1 Informal BRT (Small Scale Breach)

Medium to large scale sensitive PII Breach – the BRT is made up of a Core BRT team that may call on additional potential members depending on the size and nature of the sensitive PII breach.

7. Recovery Phase

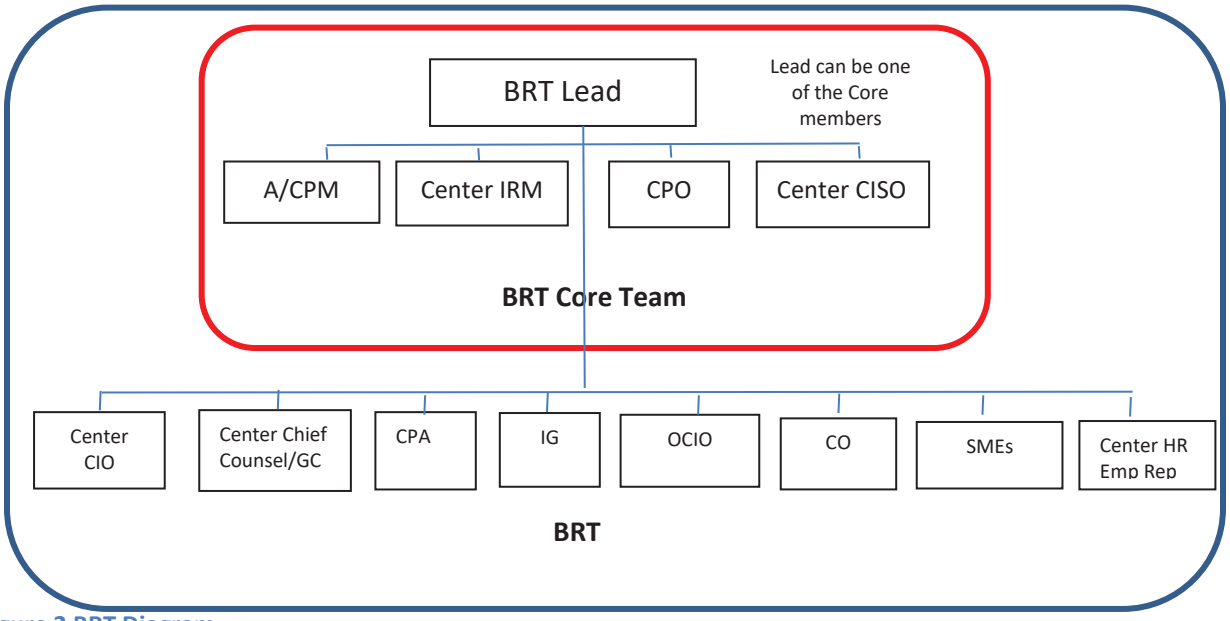

Figure 2 BRT Diagram

8. Deactivation

The BRT should be deactivated once the sensitive PII breach has been closed and the BRT Report and Lessons Learned are filed with the OCIO and the NASA Chief Privacy Officer.