NASA
Office of Inspector General

NASA's Privacy Program

December 19, 2023

IG-24-006

Office of Inspector General

To report, fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD) or visit https://oig.nasa.gov/hotline.html. You can also write to NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, D.C. 20026. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.

To suggest ideas or request future audits, contact the Assistant Inspector General for Audits at https://oig.nasa.gov/aboutAll.html.

Results in Brief

NASA's Privacy Program

December 19, 2023 IG-24-006 (A-23-09-00-MSD)

Why We Performed This Audit

NASA and other federal agencies collect, process, maintain, disseminate, and disclose personally identifiable information (PII) on employees, contractors, the public, and partners in the course of their activities. PII is information, either alone or combined with other information, that can be used to distinguish or trace an individual's identity or be linked to a specific individual, such as a name, date or place of birth, and social security number. NASA regularly uses collections of data such as applications, websites, and information systems that store and process privacy information about individuals. NASA's high-profile mission and broad connectivity with the public and outside organizations make the Agency susceptible to data breaches and the potential loss of PII. Loss of personal information maintained by or on behalf of NASA can result in substantial harm to individuals and the Agency through identity theft, economic loss, financial liability, or damage to NASA's reputation. Federal agencies are required to ensure sufficient safeguards exist to protect individuals' personal information and comply with all privacy laws, regulations, and policies when maintaining personal information.

In this audit we assessed whether NASA implemented a comprehensive privacy program to protect personal information collected, used, and maintained by the Agency. To complete this work, we interviewed NASA privacy and cybersecurity officials and information system owners. We also reviewed samples of privacy threshold analysis questionnaires and System of Records Notices; PII-related incident tickets; Breach Response Team reports; privacy training and awareness materials; and federal and NASA criteria, policies, and procedures.

What We Found

NASA has established a comprehensive privacy program that includes processes for determining whether information systems collect, store, and transmit PII; publishing System of Records Notices; and providing general privacy training to its workforce. However, NASA needs to take additional steps to better protect individuals' personal information that it collects, uses, and maintains.

NASA conducts two privacy assessments within its Risk Information Security Compliance System (RISCS): (1) the privacy threshold analysis is a questionnaire that identifies the PII collected on an application, website, or information system, and (2) the privacy impact assessment (PIA) documents that collections of data comply with federal laws and NASA policies, and that privacy risks and protections for handling personal information are evaluated. We found the Agency does not consistently document key decisions on the necessity of PIAs. Specifically, information collection owners and Agency Privacy Managers can override the requirement for a PIA if they believe it is not required by law, and not document a justification in RISCS for their decision. As a result, information on whether collections of data are compliant with applicable laws and policies may be incomplete, and NASA could fail to notify the public about the information the Agency is collecting and storing on their behalf and the safeguards that exist to protect their personal information.

NASA is also not fully utilizing its data loss prevention (DLP) capability within Microsoft's 365 platform to automatically detect incidents potentially involving PII and instead relies on users to self-report potential breaches. By establishing roles and responsibilities for the operation and maintenance of the DLP tool, including how to respond to potential breaches, NASA can enhance coordination between security and privacy officials to determine where sensitive PII resides across the Agency and develop a process for using DLP tools to protect this information. From October 2021 to March 2023, NASA's Security Operations Center logged 118 self-reported incidents suspected of or involving PII. We found the data collected for these incidents did not consistently identify the number of affected accounts, how the PII was disclosed, and root causes, nor was a risk rating assigned or lessons learned captured. While Agency security personnel complete incident information in the cybersecurity and privacy incident database, they rely on privacy officials to confirm whether the data contains PII. Without comprehensive incident details, it will be difficult for NASA to track and monitor PII incident trends and assess whether the incidents were responded to appropriately.

Further, NASA's breach response process is outlined in several documents that conflict with each other, thereby providing unclear directions. Federal guidance states agencies must implement a breach response plan, a formal document with agency policies and procedures for reporting, investigating, and managing a breach. The plan must also identify specific agency officials who make up a Breach Response Team (BRT) and their roles and responsibilities when responding to a breach. However, NASA's breach response checklist—which acts as the Agency's breach response plan—does not make clear when an incident is confirmed to be a breach and when a BRT should be formed. The checklist also provides information about breach protocols different from NASA's Information Security Incident Management handbook and privacy procedural requirements. Without a common understanding of what constitutes a breach and when to activate a BRT, NASA may not accurately report the actual number of breaches and risks mishandling incident responses where personal information may have been compromised.

Additionally, not all NASA officials with key privacy roles receive the appropriate level of privacy training. Both federal and NASA guidance requires BRTs to complete a tabletop exercise annually, which simulates an actual breach that allows BRT members to complete the breach response process and understand their roles and responsibilities. We learned BRT members did not participate in a tabletop exercise in fiscal years 2020 through 2022. NASA also does not ensure that all individuals with security and privacy roles complete privacy role-based training despite federal and NASA guidance to do so. Privacy role-based training provides learning activities to equip individuals with the knowledge and skills needed to perform the responsibilities specific to each of their roles in the organization. Only Agency Privacy Managers at NASA complete role-based training, leaving over 2,200 individuals with assigned security and privacy roles who may not be receiving the training.

What We Recommended

To strengthen NASA's privacy program to better protect personal information, we recommended NASA's Chief Information Officer and Senior Agency Official for Privacy (1) document the decision-making process between collection owners and Agency Privacy Managers to include key determinations of instances where PIAs are not required by law despite indications that one is required within RISCS; (2) establish DLP roles and responsibilities related to the oversight of and response to potential PII incidents; (3) clearly identify roles and responsibilities for tracking and documenting incident response from detection to final resolution for incidents that involve or potentially involve PII; (4) update NASA's breach response plan to clearly identify who is involved during breach responses of varying levels of severity, when a BRT should be activated, and when an incident should be categorized as a breach; (5) ensure that designated members of a BRT participate in a tabletop exercise, at least annually; and (6) require those with specific security and privacy roles to take privacy role-based training.

We provided a draft of this report to NASA management who concurred with our recommendations and described planned actions to address them. We consider management's comments responsive to Recommendations 1, 2, 3, 4, and 5; therefore, these recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions. Although the Agency also concurred with Recommendation 6, we consider the proposed actions unresponsive. Consequently, this recommendation will remain unresolved pending further discussions with the Agency.

For more information on the NASA Office of Inspector General and to view this and other reports visit https://oig.nasa.gov/.

TABLE OF CONTENTS

Acronyms

APM	Agency Privacy Manager
BRT	Breach Response Team
CPO	Chief Privacy Officer
DLP	data loss prevention
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
IMS	Incident Management System
ISO	Information System Owner
IT	information technology
NIST	National Institute of Standards and Technology
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
PTA	privacy threshold analysis
RISCS	Risk Information Security Compliance System
SOC	Security Operations Center
SORN	System of Records Notice

INTRODUCTION

Federal agencies regularly collect, process, maintain, disseminate, and disclose personally identifiable information (PII) on employees, contractors, the public, and its partners. Generally, PII refers to information, either alone or when combined with other information, that can be used to distinguish or trace an individual's identity or be linked to a specific individual. Common examples of PII include name, date or place of birth, and social security number. The need to protect personal information has become more urgent with the increase in identity theft and introduction of new and advanced technologies, such as artificial intelligence and cloud-based services, coupled with the rapidly evolving cybersecurity threat and risk landscape.[1] These technological advancements continue to give rise to additional privacy risks and pose ongoing challenges in protecting personal information.

In 2022, the Federal Bureau of Investigation reported that 58,859 victims claimed $742.4 million in total losses resulting from personal data breaches.[2] One of the biggest government data breaches in the past decade occurred at the U.S. Office of Personnel Management in 2015 where hackers stole more than 21.5 million records of current and former federal employees, much of which contained PII.[3] More recently in May 2023, the personal information of 237,000 current and former federal employees was exposed in a data breach affecting the U.S. Department of Transportation's system that supports the Federal Transit Benefit Program.[4]

NASA is not impervious to data breaches and the potential loss of personal information. The Agency's high-profile mission and broad connectivity with the public, educational institutions, research facilities, and other outside organizations make it susceptible to increased privacy risks. The loss of PII and other types of personal information maintained by or on behalf of NASA can result in substantial harm to individuals and the Agency whether through identity theft, economic loss, financial liability, or damage to NASA's reputation and culture. NASA, along with other federal agencies, are required to ensure sufficient safeguards exist for individuals' personal information and comply with all privacy laws, regulations, and policies when maintaining personal information. Additionally, for more than two decades we have identified information technology (IT) security as a top management challenge

[1] Artificial intelligence is generally thought of as the capability of a machine to imitate intelligent human behavior. Aspects of this technology are broadly used in a variety of applications ranging from medical devices to autonomous vehicles to automated maintenance for military systems. Cloud computing is the practice of using a network of remote servers hosted on the internet for centralized data access and storage to computer services or resources.

[2] According to the Federal Bureau of Investigation's Internet Crime Complaint Center, a personal data breach is a leak or spill of personal data released from a secure location to an untrusted environment or copied, transmitted, viewed, stolen, or used by an unauthorized official. These reported statistics are not specific to federal agencies. Federal Bureau of Investigation, *Internet Crime Report 2022* (accessed August 8, 2023) https://www.waterisac.org/system/files/articles/2022_IC3Report.pdf.

[3] U.S. Office of Personnel Management, *Cybersecurity Resource Center* (accessed August 2, 2023) https://www.opm.gov/about-us/our-people-organization/office-of-the-general-counsel/cybersecurity-resource-center/#url=Cybersecurity-Incidents.

[4] The Federal Transit Benefit Program provides federal employees transit benefits to encourage the use of mass transportation as the primary means of commuting from home to work to reduce their commuter carbon footprint.

at NASA.[5] While security and privacy are independent and separate disciplines, they are closely related and require a coordinated approach to identify and manage security and privacy risks.

In this audit, we assessed whether NASA implemented a comprehensive privacy program to protect personal information collected, used, and maintained by the Agency. See Appendix A for details of the audit's scope and methodology.

Background

NASA defines privacy information, or personal information, as any information that falls within the definitions of the Privacy Act of 1974 (Privacy Act), information in identifiable form, or PII as shown in Table 1.[6] PII is further classified into sensitive and non-sensitive PII. Examples of sensitive PII include driver's license or state identification numbers, social security number, biometric identifiers such as fingerprint or voiceprint, employment information (e.g., performance ratings, disciplinary actions), home address and telephone number, and financial account numbers. Non-sensitive PII includes personal identifiers such as first and last name, work location, work phone number, and work email address. Non-sensitive PII when combined with sensitive PII, such as an individual's name and social security number, result in data that is considered sensitive PII.

Table 1: NASA's Definition of Privacy Information (as of October 2023)

Privacy Information	Definition
Privacy Act Information	Any information subject to the requirements established by the Privacy Act of 1974 and NASA Privacy Act regulations, 14 C.F.R. 1212.
Information in Identifiable Form	Information in an IT system or online collection that directly identifies an individual (e.g., name, home address, social security number) or by which an agency intends to identify specific individuals in conjunction with other data elements (i.e., combination of gender, race, birth date, geographic indicator, and other descriptors).
Sensitive PII	PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
Non-sensitive PII	Information that is available through public sources, the disclosure of which cannot reasonably be expected to result in personal harm or embarrassment.

Source: NASA Office of Inspector General (OIG) presentation of Agency information.

As part of its day-to-day operations, NASA uses collections of data such as applications, websites, and information systems that store and process privacy information about individuals, from federal employees and contractors to members of the public, grant recipients, and other business partners.[7]

[5] Identification of IT security as a top management challenge can be found most recently in the NASA Office of Inspector General's (OIG) *2023 Report on NASA's Top Management and Performance Challenges* (MC-2023, November 2023). Notably, even the OIG's network is not immune to cyberattacks. In April 2022, our organization experienced a significant cyber incident that disrupted operations for months. However, no personal information was lost or compromised.

[6] Privacy Act of 1974, 5 U.S.C. § 552a (1974), as amended. The Privacy Act is the law governing the collection, maintenance, use, and dissemination of information about individuals in systems of records maintained by federal agencies.

[7] According to Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016), an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, and disposition of information. Members of the public include people or entities outside of federal government, including individual people, businesses, and associations; state, territorial, tribal, and local governments; and foreign governments and businesses.

NASA collects PII from members of the public through various applications, websites, and electronic and non-electronic records such as visitor center requests, guest account services, and media accreditations. See Figure 1 for examples of various types of collections of data that may store and process PII.

Figure 1: Examples of NASA Collections of Data

Non-Electronic Record
Electronic Record
Application
Website
Information System
Cloud System
Third-Party Website/ Application
Forms Not Affiliated with an Authorization Package

Source: NASA OIG presentation of Agency information.

When NASA uses individual identifiers like a person's name to retrieve information from a collection of data, that collection is considered a system of record. The Privacy Act requires agencies to give the public notice of their systems of records through the completion and publication of the System of Records Notice (SORN) in the Federal Register.[8] Federal agencies publish a SORN when they establish or modify a system of records to describe the existence and character of the system. Additionally, a SORN identifies the system of records, the purpose of the system, the authority for maintenance of the records, the categories of records maintained in the system and of the individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system. To meet this requirement, NASA completes a SORN for any electronic or non-electronic system of record that maintains, collects, uses, and disseminates information about individuals and routinely uses a personal identifier—such as an individual's name, home address, email address, telephone number, social security number, photograph, biometric information, or any other unique identifier that can be linked to an individual—to retrieve the information being collected.

NASA's Privacy Program and Privacy Goals

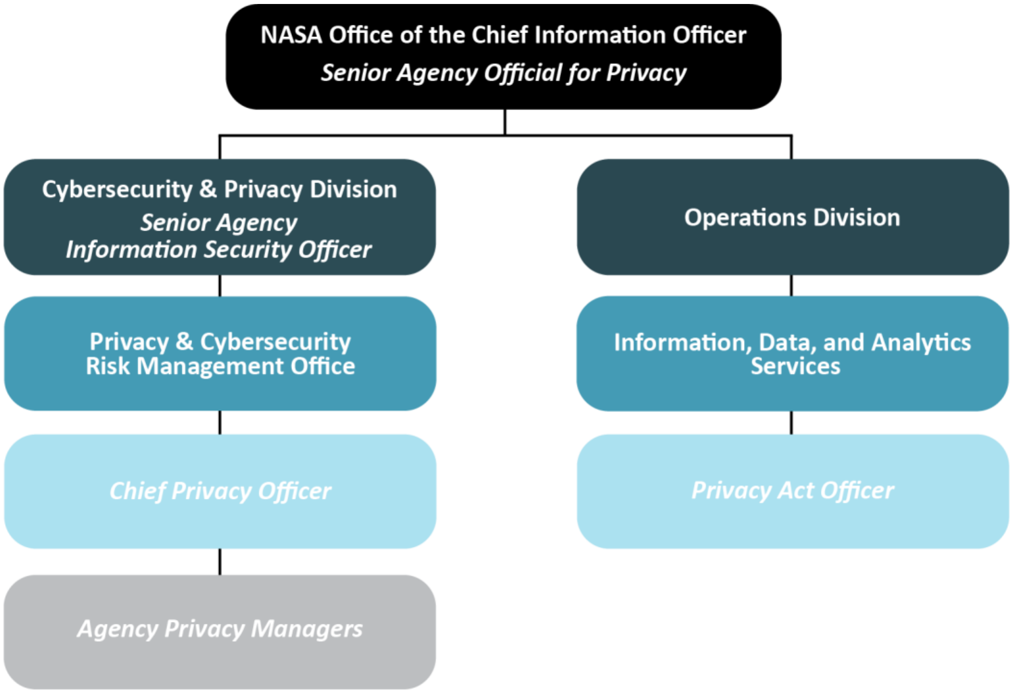
NASA's privacy program, part of the Office of the Chief Information Officer's (OCIO) Cybersecurity & Privacy Division, is responsible for ensuring privacy protections across the Agency. Overall responsibility and accountability for ensuring NASA's implementation and management of personal information protections and compliance with federal laws and regulations is delegated to the Senior Agency Official for Privacy, who is currently the Chief Information Officer. Additional privacy officials include the Chief Privacy Officer (CPO), the Privacy Act Officer, and Agency Privacy Managers (APM).[9] The CPO is responsible for responding to privacy-related actions issued by Congress and external agencies, developing privacy policies and procedural requirements, and providing final quality reviews of Agency privacy assessments. The Privacy Act Officer ensures compliance with and implements requirements of the Privacy Act including ensuring SORNs are published in the Federal Register. APMs directly support the CPO in overseeing, managing, and implementing NASA privacy policies and serve as the interface between the CPO, the Privacy Act Officer, and Center personnel on privacy matters including ensuring

[8] The Federal Register, published every federal workday by the Office of the Federal Register under the National Archives and Records Administration, is the official journal of the U.S. government. It provides the public legal notice of federal agency regulations, proposed rules, public notices, executive orders, proclamations, and other presidential documents.

[9] NASA Procedural Requirements (NPR) 1382.1B, *NASA Privacy Procedural Requirements* (July 26, 2022).

the completion of required privacy assessments. See Figure 2 for an overview of NASA's privacy program team.

Figure 2: NASA Privacy Program Team Overview (as of October 2023)


NASA Office of the Chief Information Officer
Senior Agency Official for Privacy
Cybersecurity & Privacy Division
Senior Agency Information Security Officer
Operations Division
Privacy & Cybersecurity Risk Management Office
Information, Data, and Analytics Services
Chief Privacy Officer
Privacy Act Officer
Agency Privacy Managers

Source: NASA OIG presentation of Agency information.

As a result of NASA's Mission Support Future Architecture Program, in April 2022 the privacy program transformed to an enterprise-wide operational model wherein privacy managers—previously assigned to individual NASA Centers—were consolidated under the Cybersecurity & Privacy Division and now serve as APMs providing Agency-wide privacy support as opposed to Center-specific privacy services.[10] Currently, the privacy program employs six full-time equivalents, who work as APMs, and one contractor employee.[11]

NASA's privacy program works to further the OCIO's vision and mission of securing and protecting data through the following guiding principles and goals:

- Ensure NASA only collects privacy information that is necessary for the proper performance of a NASA function and has a practical utility.
- Align NASA privacy policy, procedural requirements, and handbooks with federal requirements.
- Conduct annual reviews of collections of privacy information and reduce or eliminate unnecessary collections.

[10] The Mission Support Future Architecture Program seeks to transition mission support services traditionally managed at each NASA Center and headquarters, including IT, human capital, and financial management, to a centralized, Agency-wide operating model.

[11] A full-time equivalent is the basic measure of the levels of employment used in the budget for civil servants. It is defined as the total number of hours worked (or to be worked) divided by the maximum number of compensable hours in a fiscal year.

- Maintain and publish SORNs, NASA privacy impact assessments (PIA), and an accurate and current website privacy policy.[12]
- Maintain and publish privacy notices.
- Provide the public an opportunity to comment on NASA's privacy policies, state complaints, and seek redress.
- Notify members of the public and NASA users of any breach of their personal information collected, maintained, or stored by NASA (regardless of the data format).
- Ensure that APMs, Information System Owners (ISO), information owners, and NASA users are provided with appropriate guidance and support.

Privacy Laws, Policies, and Guidance

The Privacy Act is the principal law governing the handling of personal information in the federal government. The law requires federal agencies to follow fair information practices intended to create a foundation for trust between individuals and the government regarding use of personal data. Even still, the evolution of IT and information processing capabilities has given way to increased privacy risks resulting in the enactment of supplemental privacy-related laws, regulations, policies, and guidance for federal agencies such as the E-Government Act of 2002 (E-Government Act), the Federal Information Security Modernization Act of 2014 (FISMA), Office of Management and Budget (OMB) Circular No. A-130, and National Institute of Standards and Technology (NIST) publications.[13]

NASA has developed multiple policies, procedural requirements, and handbooks relating to the protection of personal information collected and maintained by or on behalf of the Agency. NASA's privacy policy applies to all users including civil servants and contractors who collect personal information in support of Agency projects, programs, and missions. Key aspects of the policy include protecting personal information, complying with federal laws and regulations governing management of all personal information, using the NIST Privacy Framework as a foundation to manage enterprise privacy risk, and avoiding the use of social security numbers when possible and instead relying on Agency-specific identifiers like the Universal Uniform Personal Identification Code.[14] NASA's policy is further supplemented by procedural requirements that detail the processes related to privacy management. The Agency also has various cybersecurity and privacy handbooks that provide additional implementation guidance for privacy risk management and compliance requirements.

[12] NASA's Privacy Act System of Records Notices (SORNs) (accessed August 8, 2023) can be viewed at https://www.nasa.gov/content/nasa-privacy-act-system-of-records-notices-sorns. NASA's Privacy Impact Assessment (PIA) Summaries (accessed August 2, 2023) can be viewed at https://www.nasa.gov/content/privacy-impact-assessment-pia-summaries. NASA's website privacy policy (accessed August 8, 2023) can be viewed at https://www.nasa.gov/about/highlights/HP_Privacy.html.

[13] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002); Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014); OMB A-130; NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020); and NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010). NIST is an agency of the U.S. Department of Commerce that supports organizations in better protecting individuals' privacy and helps bring privacy risk into parity with other risks such as cybersecurity and safety by engaging with stakeholders to develop privacy guidance and tools such as the NIST Privacy Framework.

[14] To enhance employee privacy while ensuring positive identification throughout NASA IT systems, NASA created the Universal Uniform Personal Identification Code—a unique number identifier—to serve as a replacement for the social security number.

Privacy Compliance Documentation

While every NASA user has the responsibility to protect PII, individuals with specific roles who are responsible for the collection of PII, such as ISOs, APMs, and the CPO, have a collective obligation to ensure privacy requirements for PII collections are met including the completion of privacy compliance documentation. To satisfy these requirements, NASA conducts two types of privacy assessments within its Risk Information Security Compliance System (RISCS)—a privacy threshold analysis (PTA) and a PIA.[15]

A PTA initiates the collection of PII into NASA's Master Privacy Information Inventory which includes a listing of all electronic and non-electronic collections of data associated with IT systems in an operation and maintenance NASA Lifecycle Status.[16] A PTA is required for all new collections of data, such as applications, websites, and information systems, as well as all preexisting collections of data that have not previously been assessed.[17] According to NASA policy, PTAs must also be conducted for all non-electronic collections of data to determine whether there are any privacy implications or other regulatory compliance requirements. Updates to PTAs are required when substantial changes are made to an application, a website, or an information system and new privacy risks are created.[18] The PTA is a questionnaire that captures the PII being collected and assists collection owners in determining whether the collection of data requires a PIA.

A PIA analyzes how PII is collected, used, stored, and protected by NASA and serves as documentation that the collection is conducted in compliance with applicable federal laws, statues, and NASA policies and procedures. The PIA examines the risk to the individual caused by the collection of information in identifiable form, which is when information is represented in a way that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. According to NASA policy, PIAs must be conducted for any new, unassessed, or substantially changed application, website, and information system that collects, maintains, or disseminates information in identifiable forms from or about members of the public.[19] PIAs are also required for information in identifiable form collections subject to the Paperwork Reduction Act as well as for pilot or third-party applications, websites, or information systems collecting PII.[20] Figure 3 provides an overview of when NASA is required to conduct PTAs and PIAs.

[15] RISCS is a system of record for the Agency's IT systems documentation. RISCS contains authorization packages which include information such as the information system security plan, privacy plan, security and privacy control assessment, and any relevant plans of action and milestones. As of January 2020, privacy assessments are stored in RISCS.

[16] NASA Lifecycle Status is based on the definition of a system development life cycle in NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy* (December 2018). A system development life cycle is the scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. According to NASA privacy officials, PTAs are often initiated during the earlier phases of a system development life cycle—initiation, development and acquisition, and implementation—but information is not collected or maintained until the IT system is in an operation and maintenance status.

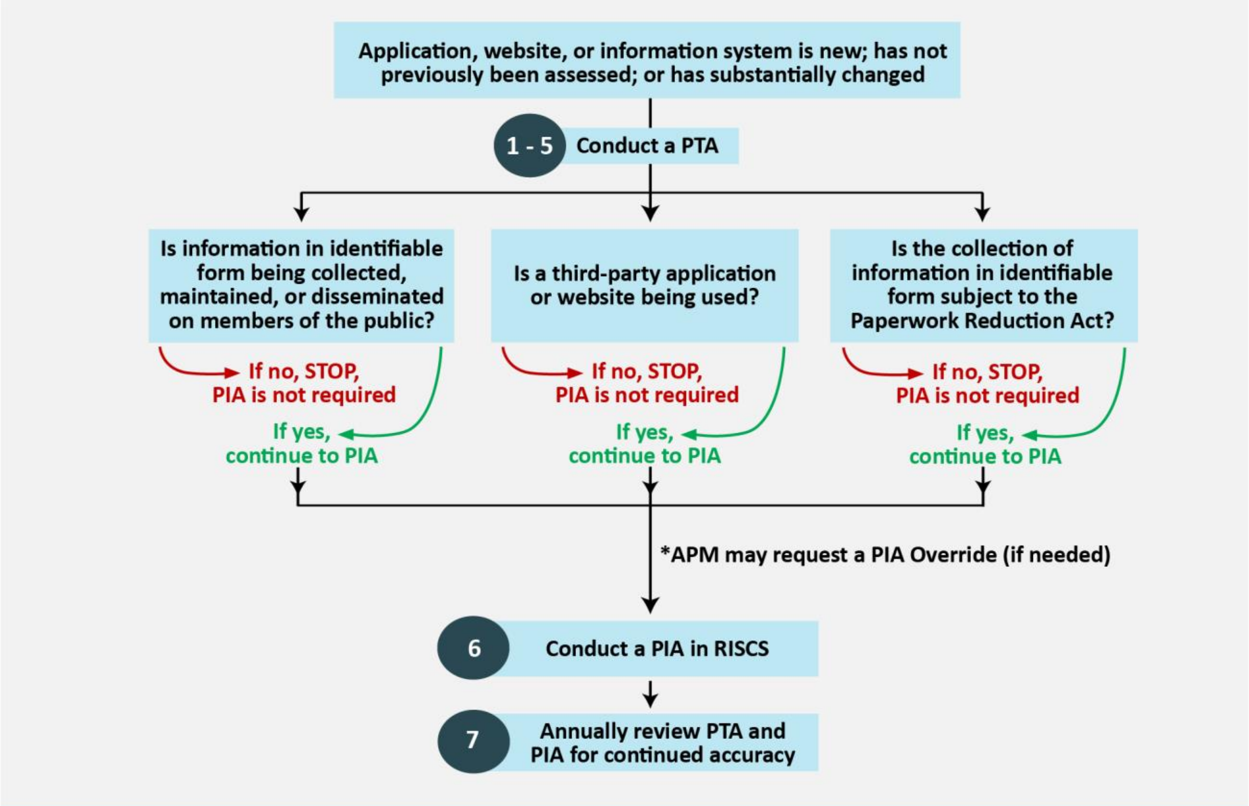
[17] NASA ITS-HBK-1382.03-01, *Privacy—Collections, PTAs, and PIAs* (March 10, 2022).

[18] Examples of substantial changes to an application, a website, or an information system include changes in how the information is being collected (e.g., forms, electronic, non-electronic), how PII is managed, who NASA collects PII from, the application of new technologies, and the duration of information retention.

[19] NASA ITS-HBK-1382.03-01.

[20] The Paperwork Reduction Act of 1995, Pub. L. No. 104-13 (1995), 44 U.S.C. § 3501 et seq., is a law governing how federal agencies collect information from members of the public.

Figure 3: When NASA Is Required to Conduct a PTA and PIA


Application, website, or information system is new; has not previously been assessed; or has substantially changed
1 - 5
Conduct a PTA
Is information in identifiable form being collected, maintained, or disseminated on members of the public?
Is a third-party application or website being used?
Is the collection of information in identifiable form subject to the Paperwork Reduction Act?
If no, STOP, PIA is not required
If yes, continue to PIA
If no, STOP, PIA is not required
If yes, continue to PIA
If no, STOP, PIA is not required
If yes, continue to PIA
*APM may request a PIA Override (if needed)
6
Conduct a PIA in RISCS
7
Annually review PTA and PIA for continued accuracy

1 **PTA is initiated in RISCS**
The following roles can initiate a PTA in RISCS: Information System Owner, Information System Security Official, Information System Security Engineer/Primary Funding Organization ISSE, Agency Privacy Manager, Agency Privacy Manager Support, Chief Privacy Office Support, Chief Privacy Officer, Information Security Privacy Officer, PTA data owner, Privacy Solution Clerk Tier 2, Center Administrator/Primary Funding Organization CA, or Center Cybersecurity Risk Manager.

2 **PTA initiator submits completed PTA to the PTA data owner for review**

3 **PTA data owner submits PTA for review to the Information System Owner**

4 **Information System Owner submits PTA for review to the Agency Privacy Manager**

5 **Agency Privacy Manager, Chief Privacy Office Support, or Chief Privacy Officer approves or rejects the PTA**

6 **PIA is conducted in RISCS if needed**
The PIA workflow process from here mimics PTA steps 2 through 5. The PIA is then reviewed in chronological order by the Office of General Counsel, Chief Privacy Officer, Senior Agency Information Security Officer, and Senior Agency Official for Privacy.

7 **Agency Privacy Managers complete the review and reduce activity**
Agency Privacy Managers initiate the annual review and reduce activity work with the appropriate Information System Owners or PTA data owners in completing the review.

Source: NASA OIG presentation of Agency information.

PTAs and PIAs are intended to demonstrate that NASA considers privacy implications from the beginning stages of a collection of data's or information system's development as well as throughout its life cycle (i.e., collection, processing, dissemination, use, storage, and disposition). Furthermore, a completed PIA provides the public notice of NASA's privacy information and risks analysis and helps promote trust between the public and NASA.[21]

Other privacy compliance assessments and documentation conducted, stored, and maintained in RISCS include SORNs, the need for which are identified by PIAs, as well as annual review and reduce activities. Per NASA's privacy handbook on reviewing and reducing PII and unnecessary use of social security numbers, annual review and reduce assessments occur during the fourth quarter of each fiscal year during which information collection owners validate or revalidate the need for their PII collections and eliminate any unnecessary holdings. Collections of PII are not authorized unless there is a clear, documented need for the information and an established authority for doing so.[22]

Ongoing Privacy Concerns

Per federal requirements, Inspectors General are required to periodically review their agencies' implementation of a privacy program and report on the results.[23] For NASA this requirement is typically met through the Office of Inspector General's (OIG) annual FISMA review, which includes tests of the Agency's privacy controls.[24] During the fiscal year 2020 FISMA evaluation, NASA OIG determined that the Agency had a maturity level of 2 (defined) out of 5 (optimized) for the data protection and privacy domain, needing improvement in areas such as data breach response. In the fiscal year 2023 FISMA evaluation, NASA's data protection and privacy domain was rated at a level 3 (consistently implemented), an improvement, but one which fell short of OMB's level 4 rating to be considered effective.[25] Additionally, the evaluation found controls, including those for PII Processing and Transparency, were not added to NASA's Information Security Continuous Monitoring Strategy; a repeat finding from the prior year.[26]

The Government Accountability Office (GAO) has also designated information security as a government-wide high-risk area for more than 25 years.[27] In 2015, GAO expanded the high-risk area to include protecting the privacy of PII and identified this area as one of four major cybersecurity challenges. To address this specific challenge, GAO identified two critical actions the federal government and other

[21] Section 208 of the E-Government Act states federal agencies shall make the PIA publicly available through the website of the agency, publication in the Federal Register, or other means. NASA's PIA summaries can be viewed at https://www.nasa.gov/content/privacy-impact-assessment-pia-summaries.

[22] NASA ITS-HBK-1382.03-01.

[23] 42 U.S.C. § 2000ee-2. The report may be incorporated into another statutorily mandated report such as the one required by the Federal Information Security Management Act of 2002. The Federal Information Security Modernization Act of 2014 amended the Federal Information Security Management Act of 2002.

[24] Privacy controls are the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

[25] NASA OIG, *NASA's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023* (IG-23-017, August 17, 2023).

[26] A continuous monitoring strategy is a method to maintain ongoing awareness of information security, vulnerabilities, and threats.

[27] GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Area*s (GAO-23-106203, April 20, 2023).

entities need to take including improving federal efforts to protect privacy and sensitive data, and appropriately limiting the collection and use of personal information and ensuring it is obtained with appropriate knowledge or consent.

Incident Response and Management

Federal policy also requires that agencies' privacy programs develop incident response and management capabilities to appropriately prepare for and respond to a loss of PII. OMB defines an incident as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system, or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[28] According to NIST guidelines, an incident response capability supports an agency's ability to respond to incidents systematically so appropriate actions are taken and helps personnel minimize loss or theft of information and disruption of services caused by incidents. Additionally, incident response allows the agency to use information gained during incident handling to better prepare it for handling future incidents and provide stronger protections for systems and data.[29]

Often, an occurrence may first be identified as an incident, but later identified as a breach once it is determined the incident involves PII. According to OMB, incidents that involve or are suspected to involve PII are considered breaches. OMB defines a breach as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where an authorized user or a person other than an authorized user accesses or potentially accesses PII for an unauthorized purpose.[30] Some common examples of a breach as defined by OMB include:

- A laptop or portable storage device storing PII is lost or stolen,
- An email containing PII is inadvertently sent to the wrong person,
- A user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual,
- An IT system that maintains PII is accessed by a malicious actor, or
- PII that should not be widely disseminated is posted inadvertently on a public website.

To effectively and efficiently respond to a breach, OMB guidance states the Senior Agency Official for Privacy must develop and implement a breach response plan—a formal document that includes the agency's policies and procedures for reporting, investigating, and managing a breach. The breach response plan must identify the specific agency officials who make up a Breach Response Team (BRT), as well as their respective roles and responsibilities when responding to a breach.[31] While a BRT is not

[28] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017).

[29] NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide* (August 2012).

[30] According to OMB M-17-12, a breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information.

[31] According to OMB, an Agency's BRT shall include the Senior Agency Official for Privacy, the Chief Information Officer or their designee, the Senior Agency Information Security Officer, legal counsel, a legislative affairs official, and a communications official. NASA furthers adds that other BRT members may include Center Chief Information Officers, Information Security Officers, the Inspector General, Contracting Officer Representatives, Human Resources officials, Office of Procurement officials, and subject matter experts as needed.

always required, it is intended to respond to and mitigate a breach by performing a breach risk assessment, providing external mitigation recommendations, and determining breach notification requirements.[32] Agency privacy program officials are responsible for determining whether a BRT should be activated.

[32] In a breach risk assessment, several factors are evaluated including the nature of the data elements breached, the number of individuals potentially affected, the likelihood the information is accessible and usable, the likelihood the breach may lead to harm, and the ability of the Agency to mitigate the risk of harm.

NASA's Privacy Program Is Comprehensive But Further Improvements Are Needed to Better Protect Personal Information

NASA has established a comprehensive privacy program that includes processes for determining whether information systems collect, store, and transmit PII; publishing SORNs; and providing general privacy training to its workforce. However, NASA needs to take additional steps to better protect individuals' personal information. Particularly, the Agency does not consistently document key decisions on the necessity of PIAs. Additionally, NASA is not fully utilizing its data loss prevention (DLP) capabilities to detect potential breaches across its network, nor does it have a clear process for deciding when to convene a BRT. Finally, not all individuals with key privacy roles receive the appropriate level of privacy training. Improvements in these areas would ensure NASA complies with federal laws when collecting PII, enhance detection and mitigation of incidents where PII is potentially compromised, and ensure NASA users are equipped with the requisite knowledge to better protect PII.

NASA Includes Key Elements in Its Privacy Program

NASA has a process to appropriately determine the risks and related compliance requirements associated with applications, websites, and information systems collecting, maintaining, and disseminating privacy information. The process results in completed PTAs, and PIAs when applicable, which are reviewed and approved by NASA's privacy managers and other privacy officials. NASA also has a process in place to annually review collections of privacy information with the intent of reducing the collection of PII—social security numbers in particular—across Agency information systems.

NASA's processes for assessing privacy requirements support the Agency's ability to notify individuals when its systems collect privacy information. To this end, NASA has a process to publish SORNs to its website and the Federal Register as well as review and update these notices as appropriate. During our review, NASA's Privacy Act Officer was actively working to update several SORNs for NASA systems that use cloud-based data solutions. According to the Privacy Act Officer, the Agency had 22 active SORNs as of April 2023. Of the 22, we reviewed 2 and noted they included required elements such as categories of individuals and records in the system and locations where data is stored. We also reviewed the template NASA uses to create their SORNs and found it included all OMB requirements.[33]

Furthermore, NASA ensures that all employees and contractors, prior to being given access to NASA systems, complete the annual Cybersecurity and Privacy Awareness Training. In accordance with NIST guidance, this training includes important topics such as the definition of PII; applicable privacy laws, regulations, and policies; and roles and responsibilities for using and protecting PII. Additionally, the Agency developed multiple methods of providing awareness materials to NASA civil servants and

[33] OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* (December 23, 2016).

contractors. For example, the OCIO maintains a SharePoint website that provides NASA employees and contractors important links and resources on protecting PII. The OCIO also uses email campaigns to warn of phishing schemes targeting NASA users that could allow unauthorized access to PII.[34]

Key Decisions on the Necessity of Privacy Impact Assessments Are Not Consistently Documented

NASA requires information collection owners, such as ISOs, to conduct PTAs within RISCS—the process which initiates the collection of PII into the NASA Master Privacy Information Inventory—at the beginning of the system, application, or information life cycle.[35] Depending on how information collection owners respond to the PTA questionnaire, the PTA will automatically indicate in RISCS whether a PIA is required.[36] PIAs serve as documentation that NASA's collections of data are conducted in compliance with applicable federal laws, statutes, and NASA policies and procedures, and that privacy risks and protections for handling personal information are evaluated.

As of April 2023, a total of 1,211 PTAs were maintained within RISCS.[37] Of these, 250 PTAs in an approved status indicated a PIA was required. Despite this requirement, we found that information collection owners and APMs can decide not to complete a PIA without documenting their decisions and related business justification in RISCS. For instance, in the sample of 35 PTAs we reviewed, 4 approved PTAs were missing their required PIAs.[38] With these 4 samples, 3 were under the purview of a single ISO and did not have approved PIAs even though it was required. The ISO could not provide an explanation as to why PIAs were not completed and approved in RISCS. However, after our request for documentation, we found a new corresponding PIA for all 3 PTAs was uploaded into RISCS but it was still being processed and discussions were ongoing as to whether the PIA was required. Regarding the fourth PTA, a PIA was required but an informal decision was made between the ISO and APM that a PIA was not needed. The ISO stated the PIA was not completed because the E-Government Act states no PIA is required where information relates to internal government operations, and the application in question only collected identity attributes on government and contractor personnel. Nevertheless, the resulting decision and business justification were not documented in RISCS.

In addition, while NASA is required to make PIAs publicly available, only 17 of 250 were posted on NASA's website as of August 2023.[39] Similar to the PTAs in our sample, it is possible that PIAs are not

[34] Phishing is a type of cyberattack where fraudulent communications are sent, usually through email and text messaging, that appear to come from a legitimate or reputable source. The attacker's goal is to steal money, gain access to sensitive data and login information, or install malware on the victim's device.

[35] According to OMB A-130, an information life cycle is made up of the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition to include destruction and deletion.

[36] Once the PTA questionnaire is completed and saved in RISCS, the system automatically scores it and determines whether a PIA needs to be completed based on select PTA responses.

[37] This includes PTAs with an overall status of draft, under review, and approved relating to IT systems with a NASA Lifecycle Status of initiation, development and acquisition, implementation, and operation and maintenance. Of the 1,211 PTAs maintained in RISCS, 1,159 were associated with IT systems in an operation and maintenance status. These numbers exclude PTAs in archive or decommission status.

[38] We reviewed a total of 35 randomly selected PTA questionnaires. During our audit, 22 of the 35 samples included PTAs in an overall status of approved. The remaining samples were in an overall status of draft or under review. Of the 22 PTA questionnaires with an overall status of approved, 6 indicated a PIA was required.

[39] NASA, *Privacy Impact Assessment Summaries*.

legally required for all 250 collections of data that may potentially collect, use, and store PII, and the E-Government Act allows for exceptions to the publication requirement.[40] However, by not documenting the outcome of the analysis—including the decision to override the indication in RISCS that a PIA is required and providing a business justification—individuals with privacy assessment responsibilities may not have complete information about whether collections of data are compliant with applicable laws and policies pertaining to PIAs. Moreover, without proper documentation and review of such key decisions, NASA may fail to publicly notify members of the public what information the Agency is collecting and storing on their behalf and the safeguards that exist to protect their personal information.

NASA privacy officials informed us that in December 2022 a new PIA override section was implemented as part of the PTA process in RISCS. The purpose of the PIA override is to improve efficiency—through automated workflow processes—and detect erroneous responses to the PTA questionnaire. According to OCIO officials, the functionality was also created in response to a previous FISMA observation pertaining to PTAs that indicate a PIA was required in instances where a PIA was not actually legally required. The PIA override within RISCS allows APMs to request an exception to the PIA required indication on PTAs, which can then only be approved by the CPO. NASA privacy officials explained that they expect widespread use of the PIA override section in the last quarter of fiscal year 2023 during which APMs will conduct annual review and reduce evaluations of all privacy assessments in RISCS. Documenting these decisions provides additional critical context and information about PII collections for individuals in roles with privacy assessment responsibilities. This is especially important in times of transition such as the current Agency-wide Mission Support Future Architecture Program transformation where privacy-related roles and responsibilities are being centralized across the Agency.

NASA Is Not Fully Utilizing Its Privacy Incident Detection Capabilities

NASA has a DLP capability within Microsoft's 365 platform to automatically detect incidents potentially involving PII across the Agency.[41] While deployment of the DLP capability is still ongoing, NASA has not fully established roles and responsibilities for the operation and maintenance of the DLP tool, including responding to potential breaches—incidents that involve PII—when identified. Instead, the Agency is limited in its incident response and management by relying on users to self-report potential breaches. An example of self-reporting is when a NASA user sends PII in an unencrypted email to a recipient and subsequently reports the incident to NASA's Security Operations Center (SOC) for containment and mitigation.[42]

Microsoft 365 enables organizations to implement a DLP capability by defining and applying varying DLP policies—automated rules to monitor and potentially block prohibited user activity such as inappropriate sharing of sensitive PII through email. Notably, one FISMA reporting metric seeks to

[40] The requirement to make PIAs publicly available through the Agency's website or publication in the Federal Register may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

[41] DLP capabilities are designed to detect and prevent the unauthorized use and transmission of sensitive information in an IT system.

[42] NASA's SOC provides 24-hour incident response and management and centralized oversight of the Agency's IT threat assessment. The SOC is generally accountable for monitoring and detecting suspicious events, collecting and analyzing information, identifying affected NASA resources, declaring an incident and activating an incident response team, and conducting root cause analyses of incidents.

measure the extent to which an organization has implemented security controls to prevent data exfiltration such as utilizing DLP capabilities to monitor outbound communications traffic and detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII.[43]

According to an OCIO official, the Microsoft 365 DLP tool is configured and ready for implementation into the SOC's incident response and management process but requires additional approvals from stakeholders. In 2019, NASA attempted to implement Microsoft's 365 DLP tool but the software license at the time limited the Agency's ability to fine tune its DLP policies resulting in an overwhelming number of false positives—an alert that incorrectly indicates a vulnerability is present. NASA SOC and OCIO officials explained that at that time the SOC was not equipped to manage the increase in their workload, respond, and act on the large number of false positives for PII-related DLP alerts.

In progressing with the upgraded DLP capability, NASA will need to establish a process, including roles and responsibilities, for responding to DLP alerts relating to potential breaches and how PII-related incidents will be communicated to relevant stakeholders. OCIO personnel are working towards implementation, which will involve coordinating multiple stakeholders across the organization. When considering appropriate roles and responsibilities, it is important to note that OMB's fiscal year 2023 FISMA guidance emphasizes the importance of improving security-privacy coordination and that such coordination is essential to managing security and privacy risks, including incident response.[44]

By not fully utilizing the DLP capability and relying on users to self-report potential breaches, NASA is not benefiting from resources that could minimize loss or theft of personal information and increases its risk of not identifying and responding to intentional or unintentional mishandling of PII. This could result in substantial harm to individuals and the Agency whether through identify theft, economic loss, financial liability, or damage to NASA's reputation and culture. By establishing DLP roles and responsibilities, NASA can enhance coordination between security and privacy officials to determine where sensitive PII resides across NASA and identify the process for using DLP tools to protect this information.

Data Elements Related to Incidents Involving PII Are Incomplete

Between October 2021 and March 2023, the SOC logged 118 self-reported incidents involving or suspected of involving PII in its Incident Management System (IMS).[45] The IMS is an electronic database used to track and document cybersecurity and privacy incidents. The system has fields to capture standard data elements (e.g., the number of accounts potentially affected by the incident, root causes, and lessons learned), including a section for documenting information pertaining to potential breaches. However, we did not find that any of the standard IMS fields captured whether incidents were confirmed as having PII and whether the PII was sensitive. Further, NASA does not enforce the completion of IMS fields thereby creating inconsistencies in the documentation of potential breaches.

[43] According to NIST, a security control is a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. Additionally, NIST defines exfiltration as the unauthorized transfer of information from a system.

[44] OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022).

[45] The SOC logs all incidents, including those involving or suspected of involving PII, in the IMS.

For the 118 self-reported incidents the SOC categorized as involving or potentially involving PII, we found the IMS data was incomplete.[46] Specifically:

- 90 did not identify the number of affected accounts,
- 54 did not include how PII was disclosed,
- 20 were not assigned a risk rating,
- 117 did not identify a root cause, and
- All 118 failed to capture lessons learned.

NIST guidance states that organizations should define a standard set of incident-related data elements to be collected for each incident to facilitate a more effective and consistent incident handling process.[47] Further, NIST recommends that every step taken from the time the incident is detected to its final resolution should be documented. According to OCIO officials, not all IMS fields are mandatory and incident responders generally have flexibility in determining what fields to complete within the IMS. While NIST guidance allows for this flexibility, NASA's own incident response handbook outlines an incident follow-up phase designed to identify the root cause of incidents and implement lessons learned from incidents; a task difficult to perform without complete incident information.[48] While SOC personnel are primarily responsible for completing incident information in IMS, they rely on privacy officials for certain information, specifically to confirm whether data is considered PII. According to SOC officials, improvements could be made to ensure this information is captured in IMS.

Complete data elements for incidents involving or potentially involving PII can lead to more effective lessons learned discussions between the privacy program and SOC officials. Such communication and coordination would enhance NASA's ability to identify incident characteristics that may indicate systemic security weaknesses, recurring threats, and changes in incident trends. Additionally, improving the quality of PII-related incident documentation can provide the Agency with relevant information to evaluate incident details to enhance its ongoing DLP capabilities. Without comprehensive incident details, it will be difficult for NASA to track and monitor trends related to PII incidents and assess whether these types of incidents were responded to appropriately.

Breach Response Team Activation Procedures Are Unclear

NASA's process for responding to a suspected or confirmed breach is dispersed among several documents that conflict with each other, making it unclear when a BRT should be convened. OMB guidance states that to effectively and efficiently respond to a breach, agencies must develop and implement a breach response plan—a formal document that includes the agency's policies and procedures for reporting, investigating, and managing a breach.[49] The breach response plan must also

[46] The SOC provided us with a report of incidents that were categorized as containing or potentially containing PII for the period October 1, 2021, through March 31, 2023.

[47] NIST Special Publication 800-61 Rev. 2.

[48] NASA ITS-HBK-2810.09-02A, *Incident Response and Management: NASA Information Security Incident Management* (November 6, 2019).

[49] OMB M-17-12.

identify the specific agency officials who make up a BRT, as well as their respective roles and responsibilities when responding to a breach. According to NASA privacy officials, some breaches require a BRT while others do not. Although OMB guidance gives agencies the flexibility to develop and tailor their breach response plans to best suit their environment, NASA's current policies do not make clear its process for responding to breaches, including when an incident should be considered a breach. Specifically, we were unable to determine how NASA decided whether a breach required the activation of a BRT.

NASA Procedural Requirements (NPR) for privacy state the mechanism for responding to a confirmed moderate or high-risk breach is a "privacy BRT," which is convened within 24 hours of the incident.[50] While the NPR specifies a BRT is convened based on the severity of a confirmed breach, it is not clear what criteria constitutes a breach of moderate or high risk. Further, in accordance with the NPR, a BRT is convened when a breach of sensitive PII meets the threshold outlined in NASA's information security handbooks. However, this threshold is not uniformly defined within the Information Security Incident Management or Privacy Incident Response handbooks.[51]

According to NASA privacy officials, the breach response checklist found in the Privacy Incident Response handbook acts as the Agency's breach response plan. The procedures in the checklist give incident responders and APMs guidance on responding to breaches. However, the ordering of tasks laid out in the checklist does not make it clear when an incident is confirmed to be a breach and when a BRT should be formed. While the checklist states a BRT is convened due to a suspected or confirmed breach of PII, NASA's Information Security Incident Management handbook in contrast states a BRT is activated upon determination that sensitive PII is involved in an incident.[52] Privacy officials explained they are in the process of updating the NPR for privacy to align with current OMB and NIST guidance and remove outdated references. See Table 2 for an overview of the differences in NASA's BRT activation procedures.

Table 2: Differences in NASA's Breach Response Team Activation Procedures

Procedure	Privacy Incident Response Handbook/Breach Response Checklist (Breach Response Plan)	Information Security Incident Management Handbook	NASA Procedural Requirements for Privacy
A BRT is convened when there is…	A ***suspected*** or confirmed breach of PII	***Confirmed sensitive*** PII involved in an incident	A ***confirmed moderate or high-risk breach;*** a breach of ***sensitive*** PII that meets the threshold outlined in the related handbooks

Source: NASA OIG presentation of Agency information.

While NASA's breach response procedures rely on individuals using a common definition of breach, the Agency has not clearly defined the term throughout its procedures. For fiscal year 2022, NASA reported 53 breaches within the Agency despite only activating 3 BRTs during this same period. For example, one

[50] NPR 1382.1B.

[51] NASA ITS-HBK-1382.05-01, *Privacy Incident Response: Breach Team Response Checklist* (July 14, 2022) and NASA ITS-HBK-2810.09-02A.

[52] NASA ITS-HBK-2810.09-02A.

BRT was formed to mitigate personal information accidentally being published to a public-facing NASA website while another BRT mitigated an email containing sensitive personal information that was both unencrypted and sent to unintended NASA and non-NASA users.[53] However, without clear procedures, including a common understanding of what constitutes a breach, NASA may not be accurately reporting the number of breaches within the Agency and risks mishandling the response to other incidents where individuals' personal information may have been compromised.

NASA Excludes Individuals with Key Privacy Roles from Training

Breach Response Team Designated Agency Officials Do Not Receive Required Training

NASA's designated BRT officials do not receive required annual training. According to OMB guidance, a BRT is the group of officials that may be convened to respond effectively and efficiently to a breach. At NASA, each breach may necessitate the designation of different Agency officials to convene a BRT depending on the nature and severity of a breach and the Centers affected. The NPR for privacy requires members of a BRT to participate in BRT training and exercises annually. NASA's Privacy Awareness and Training handbook further defines that BRT training must include a tabletop exercise, while OMB guidance states the Senior Agency Official for Privacy shall periodically, but not less than annually, convene the agency's BRT to hold a tabletop exercise.[54]

According to OMB guidance, a tabletop exercise can test the effectiveness of an incident response plan by simulating an actual breach. It provides a scenario that allows BRT members to complete the breach response process and understand their roles and responsibilities within that process. Further, this exercise is used to practice a coordinated response to a breach, identify potential weaknesses in an agency's response capabilities, and further refine and validate the breach response plan. Notably, testing breach response plans is an essential part of risk management and breach response preparation. In an annual report required by FISMA, NASA reported that BRT members did not participate in a tabletop exercise in fiscal years 2020 and 2021, and according to the CPO, they also did not participate in fiscal year 2022.[55]

The CPO further explained that NASA meets the intent of the required BRT tabletop exercise and training through the participation of APMs in an actual breach. In their view, the OMB requirement implies that as long as the APMs participate in an actual breach NASA does not have to complete the other requirements. In addition, the CPO stated that an overview of the breach for every BRT convened is provided during weekly or ad hoc meetings for APMs. While we agree that participating in a breach and providing an overview of BRTs to the APMs is beneficial, APMs are not the only members of a BRT.

[53] In both examples, a BRT documented details of each incident which included a timeline, a determination of risk of harm, and whether to notify or provide identity protection services to those affected.

[54] NASA ITS-HBK-1382.07-01, *Privacy Awareness and Training* (November 19, 2018) and OMB M-17-12.

[55] FISMA requires agencies to submit an annual report with descriptions of the agency's implementation of the requirements in OMB M-17-12 including confirming that BRT members participated in at least one tabletop exercise during the reporting period.

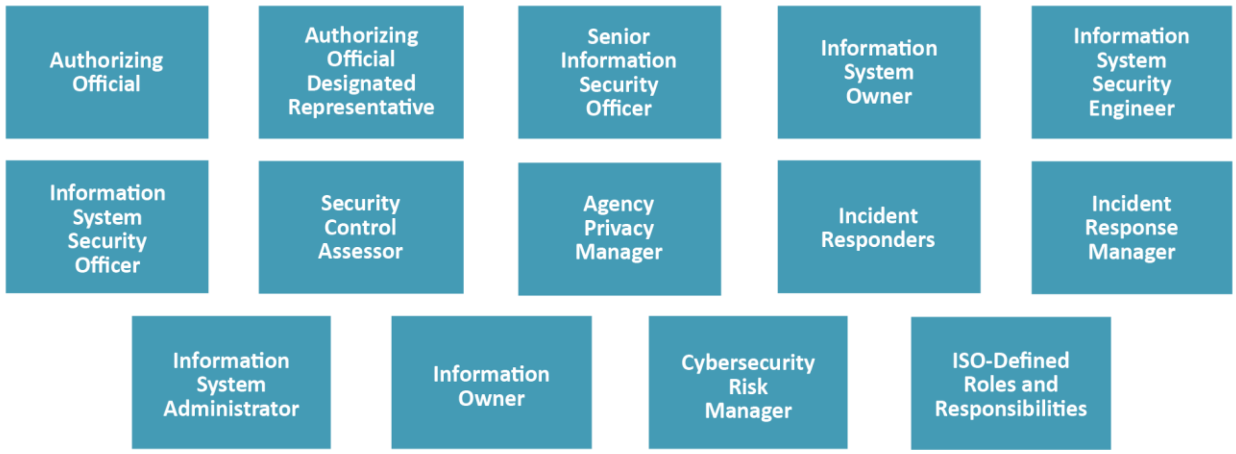
BRT training equips individuals with the requisite knowledge to efficiently respond to breaches. By not completing these requirements, designated BRT members could lack the awareness and skills necessary to carry out their assigned responsibilities during a breach resulting in negligence or nonperformance of key processes for notifying individuals, remediation activities, and documentation requirements.

Security and Privacy Officials Do Not Receive Privacy Role-Based Training

NASA does not require all individuals assigned security and privacy roles to complete privacy role-based training. With role-based training, individuals are provided a set of learning activities that equip them with the knowledge, skills, and abilities needed to perform the responsibilities specific to each of their roles in the organization. According to the CPO, the only required privacy role-based training is the Center Privacy Manager Training which is taken by the APMs annually. However, the CPO only informally requires the APMs to take this course, which is self-assigned by the learner and therefore not mandatory within NASA's training platform. While other crucial roles such as ISOs and information system security officers have role-based training available to them, it does not include a privacy component despite them having significant responsibilities for creating, maintaining, and updating privacy assessments within RISCS.

OMB guidance states that role-based security and privacy training should be provided to employees and contractors with assigned security and privacy roles and responsibilities, including managers, before authorizing access to federal information or information systems or performing assigned duties.[56] Further, NIST guidance states that role-based security and privacy training should be provided to personnel as defined by each organization. In response, NASA requirements state that role-based security and privacy training shall be provided to the roles outlined in Figure 4 annually.[57]

Figure 4: NASA Roles Required to Take Privacy Role-Based Training (as of October 2023)



Authorizing Official

Authorizing Official Designated Representative

Senior Information Security Officer

Information System Owner

Information System Security Engineer

Information System Security Officer

Security Control Assessor

Agency Privacy Manager

Incident Responders

Incident Response Manager

Information System Administrator

Information Owner

Cybersecurity Risk Manager

ISO-Defined Roles and Responsibilities

Source: NASA OIG presentation of Agency information.

[56] OMB A-130.

[57] NASA Technical Specification NASA-SPEC-2661.ODVr5 v1.2, *NASA's Organization-Defined Values for NIST Special Publication 800-53 Revision 5* (April 24, 2023).

According to Agency privacy officials, only APMs complete role-based privacy training. Since the APM is responsible for overseeing, managing, and implementing privacy-related activities throughout the Agency, privacy officials believe it is the responsibility of the APM to provide guidance to the other individuals with security and privacy roles.

The goal of role-based privacy training is to build knowledge and skills that will enable individuals with privacy responsibilities to protect PII. By not ensuring that all individuals with assigned security and privacy roles and responsibilities, such as ISOs, obtain role-based privacy training, NASA may not be equipping individuals with the requisite knowledge and skills needed to perform privacy duties specific to each of their roles. Additionally, users in roles such as an ISO or information system security officer may not have the appropriate awareness and training to adequately identify collections of data that store and process PII and to understand when a privacy assessment is required. As of September 2023, 2,289 civil servants and contractors have assigned security and privacy roles and responsibilities within RISCS who may not be receiving role-based privacy training.[58]

[58] The OIG calculated the number of individuals based on a listing of all active users with an assigned and provisioned RISCS user role that generally maps to NASA's requirements. This calculation excludes duplicate users who may be assigned more than one role in RISCS.

OTHER MATTERS OF INTEREST

Prior to RISCS, NASA's privacy program used the Privacy & Controlled Unclassified Assessment Tool to conduct its privacy-related activities. However, the transition from the Privacy & Controlled Unclassified Assessment Tool to RISCS in January 2020 may have resulted in the loss of initial PTA compliance documentation.[59] During our sample review of 35 PTA questionnaires, we were unable to locate an initial PTA within RISCS for 18 of the 22 questionnaires with an overall status of approved. Through discussions with APMs and ISOs, we learned that preexisting PTAs in the Privacy & Controlled Unclassified Assessment Tool may have been recreated in RISCS after the transition. For these 18 PTAs, we found the date stamps for when the PTAs were created in RISCS did not precede January 2020 when the transition occurred. Therefore, we were unable to determine whether a PTA was conducted at the beginning of the information life cycle and before the information system received its initial authorization to operate.[60] We noted that for each of the 18 approved PTAs there was a current PTA within RISCS.

[59] Initial PTA refers to the first PTA created prior to an IT system's original operational status.

[60] According to OMB A-130, an authorization to operate refers to the official management decision given by a senior federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.

CONCLUSION

Considering the rapid advancement of technology, collection of privacy data, and the federal government's heightened susceptibility to breaches, the protection of personal information maintained by government agencies has become increasingly important. NASA, in turn, must ensure it is protecting individuals' personal information given its high-profile missions and widespread public recognition. While the Agency has implemented a comprehensive privacy program to protect PII, several areas can be further improved. For example, the Agency would benefit from documenting instances where a PIA may not be legally required as it would assist those with privacy assessment responsibilities in executing their duties. Establishing clear roles and responsibilities around DLP and breach responses will allow the Agency to better protect PII and accurately track the number of breaches occurring within NASA. Ensuring the appropriate individuals receive breach response and privacy role-based training will bolster the knowledge and skillset of the Agency's workforce and better equip individuals to proactively protect PII and efficiently respond to suspected or confirmed breaches. Doing so will enable NASA to better protect individuals' PII from loss and limit the potential harm to individuals and the Agency whether through identity theft, economic loss, financial liability, or damage to its reputation and culture.

Recommendations, Management's Response, and Our Evaluation

To strengthen NASA's privacy program to better protect personal information, we recommended NASA's Chief Information Officer and Senior Agency Official for Privacy:

1. Document the decision-making process between collection owners and Agency Privacy Managers to include key determinations of instances where privacy impact assessments are not required by law despite indications that one is required within RISCS.
2. Establish data loss prevention roles and responsibilities related to the oversight of and response to potential personally identifiable information incidents.
3. Clearly identify roles and responsibilities for tracking and documenting incident response from detection to final resolution for incidents that involve or potentially involve personally identifiable information.
4. Update NASA's breach response plan to clearly identify who is involved during breach responses of varying levels of severity, when a Breach Response Team should be activated, and when an incident should be categorized as a breach.
5. Ensure that designated members of a Breach Response Team participate in a tabletop exercise, at least annually.
6. Require those with specific security and privacy roles to take privacy role-based training.

We provided a draft of this report to NASA management who concurred with our recommendations and described planned actions to address them. We consider management's comments responsive to Recommendations 1, 2, 3, 4, and 5; therefore, these recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions. Although the Agency also concurred with Recommendation 6, we consider the proposed actions unresponsive. The Agency stated that it will update NASA-Spec-2661, *NASA's Organization-Defined Values for NIST Special Publication 800-53*, to clearly identify privacy-role based training requirements for specific security and privacy roles. While we appreciate the Agency's review of its requirements, it is unclear whether those updates will ensure individuals with security and privacy roles are required to take privacy role-based training. During our review, NASA's requirements outlined 14 distinct security and privacy roles—with 2,289 civil servants in those roles as of September 2023—required to take privacy role-based training, yet only those designated as Agency Privacy Managers complete role-based privacy training. Consequently, this recommendation will remain unresolved pending further discussions with the Agency.

Management's comments are reproduced in Appendix B. Technical comments provided by management and revisions to address them have been incorporated as appropriate.

Major contributors to this report include Tekla Colón, Mission Support Audits Director; Yessica Nelson, Assistant Director; Anu Bakshi; Daniel Fenzau; and Aleisha Fisher. Cody Bryant and Daniel Mills provided sampling and data mining assistance, and Sashka Mannion provided legal assistance. Lauren Suls provided editorial and graphics assistance.

If you have questions about this report or wish to comment on the quality or usefulness of this report, contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202-358-1543 or laurence.b.hawkins@nasa.gov.

PAUL MARTIN

Digitally signed by PAUL MARTIN
Date: 2023.12.15 10:26:16 -05'00'

Paul K. Martin
Inspector General

Appendix A: Scope and Methodology

We performed this audit from February 2023 through November 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of this audit included assessing NASA's overall privacy program and related management policies and practices. We assessed whether NASA implemented a comprehensive privacy program to protect personal information collected, used, and maintained by the Agency. Specifically, we evaluated (1) how NASA manages storage, transmission, and reduction of personal information across NASA systems and ensures privacy-related analyses are completed as required; (2) what processes are in place to review, approve, and publish SORNs; (3) what incident response measures are in place to notify individuals of loss of personal information; and (4) whether NASA is administering the appropriate level of privacy awareness training to employees and contractors.

To determine how NASA manages personal information across NASA systems and whether NASA is completing privacy assessments as required, we interviewed Agency privacy officials such as the CPO, APMs, a Center Chief Information Security Officer, OCIO officials responsible for RISCS, and ISOs. Additionally, we tested a non-statistical random sample of 35 PTA questionnaires from RISCS for various compliance and control attributes. Our audit population from which we sampled included 1,211 PTAs in draft, under review, and in an approved status relating to IT systems with a NASA Lifecycle Status of development and acquisition, implementation, initiation, and operation and maintenance. Of those PTAs, 1,159 were associated with IT systems in an operation and maintenance status. These numbers exclude PTAs in an archive or decommission status. Our sample of 35 PTAs included a stratified random sample of 22 PTAs in an approved status, 6 PTAs in a draft status, and 2 PTAs in an under review status. We also judgmentally selected 5 PTAs associated with an external system—collections of data maintained by a system outside of NASA’s purview but subject to the same privacy requirements as a NASA system. We judgmentally selected the sample size of each stratum to achieve audit and sampling objectives. Based on our sampling methodology, we cannot project the results of our sample testing to the overall population of 1,211 PTAs.

We reviewed RISCS documentation for each sampled PTA to determine whether the information system was categorized at a moderate or high impact level; the PTA was reviewed and approved prior to the information system’s authorization or reauthorization; the PTA was updated as a result of substantial changes; a required PIA was conducted prior to the collection of PII, cited legal authorities, and made publicly available; an annual review and reduce activity was completed timely; and the PTA listed an active and current ISO.

To determine whether NASA is reviewing and publishing SORNs, we interviewed NASA privacy officials and the Privacy Act Officer to gain an understanding of how NASA identifies the need for a SORN and to obtain an authoritative list of NASA systems of record. We obtained a listing of NASA’s 22 active SORNs as of April 24, 2023, from the Privacy Act Officer and compared them to published SORNs on NASA’s website. Of these 22 SORNs, we reviewed copies of 2 from the Federal Register to determine whether they included fields required by law. We also compared the template NASA uses to create their SORNs to OMB's Office of the Federal Register SORN template for required elements.

To determine whether the Agency has incident response measures in place to notify individuals of the potential loss of their personal information, we interviewed NASA privacy, SOC, and cybersecurity officials to gain an understanding of how NASA identifies and responds to potential breaches and how NASA decides when to notify individuals of suspected or confirmed breaches. We analyzed 118 incident tickets in the IMS that were categorized as potentially involving PII for the period October 1, 2021, through March 31, 2023. For those incident tickets, we reviewed select fields designed to capture PII incident details to determine what types of incident information was recorded. We also reviewed two examples of BRT reports provided by privacy officials to understand what information BRTs document including how they measured risk of harm to individuals and whether to offer services such as identity monitoring. Finally, to determine whether NASA had a process in place to notify individuals of loss of personal information, we interviewed privacy officials as well as those from NASA's Office of General Counsel to gain an understanding of the notification process. We reviewed notification letter templates and examples of actual notifications and remediation efforts documented in BRT reports.

To determine whether NASA administered the appropriate level of privacy awareness and role-based training, we interviewed the CPO as well as NASA's IT Security Awareness and Training Center personnel to gain an understanding of how training requirements are determined, enforced, and tracked, and what privacy trainings are required for civil servants and contractors. We also reviewed privacy training course materials to determine whether required privacy topics were included and other role-based training to determine if any supplemental privacy topics were included. Additionally, we reviewed NASA's privacy awareness materials such as newsletters and additional NASA resources. To estimate the number of users—civil servants and contractors—with assigned security and privacy roles and responsibilities within RISCS that may not be receiving role-based privacy training, we identified RISCS user roles that generally map to *NASA's Organization-Defined Values for NIST Special Publication 800-53 Revision 5* for privacy role-based training requirements. NASA officials provided us with a listing of users in those roles as of September 22, 2023. We then excluded all users with an inactive status or non-provisioned role, and users who may be assigned more than one RISCS role.

Finally, we reviewed federal and NASA criteria, policies, procedures, and supporting documentation; NIST guidance; prior audit reports; external reviews; and other documents related to NASA's privacy program.

Assessment of Data Reliability

We relied upon PTA data from RISCS and incident data from the IMS as part of performing this audit. We assessed the reliability of the PTA data within RISCS by (1) performing electronic testing for missing data, outliers, and anomalies; (2) reviewing existing information about the data and NASA documentation on the system that produced them; (3) interviewing Agency officials knowledgeable about the data; and (4) reconciling the data to NASA's Master Privacy Information Inventory. We assessed the reliability of IMS data by (1) analyzing select data fields for completeness, duplicate records, valid date stamps, and indications that the data related to PII incidents, and (2) interviewing Agency officials knowledgeable about the data. While we determined the PTA and incident ticket data we used from RISCS and IMS, respectively, was sufficiently reliable for the purposes of our audit objective, we identified risks to the completeness of the data as discussed in the report.

Review of Internal Controls

We assessed internal controls and compliance with laws and regulations to determine whether NASA had a comprehensive privacy program. Specifically, we assessed the control activities component of internal controls including the principles relating to the design of control activities to achieve objectives and respond to risks and implementing control activities through policies. Control weaknesses are identified and discussed in this report. Our recommendations, if implemented, will improve those identified weaknesses. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Prior Coverage

During the last 5 years, NASA OIG issued eight reports containing some relevance to the subject of this audit. Additionally, GAO has issued two ancillary reports of interest to this topic. Unrestricted reports can be accessed at https://oig.nasa.gov/audits/auditReports.html and https://www.gao.gov, respectively.

NASA Office of Inspector General

NASA's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023 (IG-23-017, August 17, 2023)

NASA Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2022 (IG-23-006, December 19, 2022)

NASA's Cybersecurity Readiness (IG-21-019, May 18, 2021)

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation—A Contractor-Operated Communications System (IG-21-015, March 24, 2021)

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation—A Center Command and Control System (IG-21-014, March 2, 2021)

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation—A Center Communications System (IG-21-013, February 16, 2021)

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation—An Agency Common System (IG-21-010, December 22, 2020)

Cybersecurity Management and Oversight at the Jet Propulsion Laboratory (IG-19-022, June 18, 2019)

Government Accountability Office

High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas (GAO-23-106203, April 20, 2023)

Privacy: Dedicated Leadership Can Improve Programs and Address Challenges (GAO-22-105065, September 22, 2022)

Appendix B: Management’s Comments

National Aeronautics and Space Administration

Mary W. Jackson NASA Headquarters
Washington, DC 20546-0001

Reply to Attn of: Office of the Chief Information Officer

TO: Acting Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Agency Response to OIG Draft Report, “NASA's Privacy Program” (A-23-09-00-MSD)

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, “NASA's Privacy Program” (A-23-09-00-MSD), dated November 8, 2023.

In the draft report, the OIG makes six recommendations to the Chief Information Officer and Senior Agency Official for Privacy designed to strengthen NASA's privacy program to better protect personal information.

Specifically, the OIG recommends the following:

Recommendation 1: Document the decision-making process between collection owners and Agency Privacy Managers to include key determinations of instances where privacy impact assessments are not required by law despite indications that one is required within RISCS.

Management’s Response: NASA concurs. The following document:

Cybersecurity Infrastructure (CSI), Risk Information Security Compliance System (RISCS), Process (PR), and External (EX) (CSI-RISCS-PR-EX-000324), *RISCS Assessment and Authorization RISCS Operations Guide (A&A ROG)* will be updated to ensure that “Privacy Impact Assessment (PIA) override request” document both key determinations and the rationale for requested override in instances where PIAs are not required by law despite indications that one is required within the RISCS.

Estimated Completion Date: September 30, 2024.

Recommendation 2: Establish data loss prevention roles and responsibilities related to the oversight of and response to potential personally identifiable information incidents.

Management’s Response: NASA concurs. Preliminary roles and responsibilities related to Data Loss Prevention (DLP) management and DLP incident response have been defined and communicated between the NASA Privacy Team, the NASA Security Operations Center (SOC), and NASAs Cybersecurity Engineering Team. Cybersecurity Privacy Division CSPD leadership will review and approve roles and responsibilities subsequently DLP will be implemented.

Estimated Completion Date: March 31, 2024.

Recommendation 3: Clearly identify roles and responsibilities for tracking and documenting incident response from detection to final resolution for incidents that involve or potentially involve personally identifiable information.

Management's Response: NASA concurs. ITS-HBK-1382.05-01, *Privacy Incident Response and Management: Breach Response Team Checklist* will be updated to identify and define roles and responsibilities for tracking and documenting incident response from detection to final resolution for incidents that involve or potentially involve personally identifiable information.

Estimated Completion Date: September 30, 2024.

Recommendation 4: Update NASA's breach response plan to clearly identify who is involved during breach responses of varying levels of severity, when a Breach Response Team should be activated, and when an incident should be categorized as a breach.

Management's Response: NASA concurs. ITS-HBK-1382.05-01, *Privacy Incident Response and Management: Breach Response Team Checklist* will be updated to clearly convey the following:

1) When an incident should be categorized as a breach.
2) When a formal Breach Response Team (BRT) should be convened.
    a. Identify BRT participants and level of involvement.
    b. Clarify roles of BRT participants.

Estimated Completion Date: September 30, 2024.

Recommendation 5: Ensure that designated members of a Breach Response Team participate in a tabletop exercise, at least annually.

Management's Response: NASA concurs. NASA Procedural Requirement (NPR) 1382.1, *NASA Privacy Procedural Requirements* will be updated to ensure that designated core BRT members participate annually in an Agency Incident Response Assessment conducted by the CSPD.

Estimated Completion Date: September 20, 2025.

Recommendation 6: Require those with specific security and privacy roles to take privacy role-based training.

Management's Response: NASA concurs. NASA will update NASA-Spec-2661, *NASA's Organization -Defined Values for NIST Special Publication 800-53* to clearly identify privacy role-based training requirements for specific security and privacy roles.

Estimated Completion Date: September 30, 2024.

We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Matthew Degrave at (757) 864-6838.

RICHARD
RODGERS

Digitally signed by RICHARD
RODGERS
Date: 2023.12.12 07:27:13 -06'00'

Jeff Seaton
Chief Information Officer

APPENDIX C: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Associate Administrator
Associate Administrator for Technology, Policy, and Strategy
Chief of Staff
Chief Information Officer
Chief Privacy Officer

Non-NASA Organizations and Individuals

Office of Management and Budget
Deputy Associate Director, Climate, Energy, Environment and Science Division

Government Accountability Office
Director, Contracting and National Security Acquisitions

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies

Senate Committee on Commerce, Science, and Transportation
Subcommittee on Space and Science

Senate Committee on Homeland Security and Governmental Affairs

House Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies

House Committee on Oversight and Accountability
Subcommittee on Government Operations and the Federal Workforce

House Committee on Science, Space, and Technology
Subcommittee on Investigations and Oversight
Subcommittee on Space and Aeronautics

(Assignment No. A-23-09-00-MSD)