



Privacy Impact Assessment (PIA)

PIA Entry Name: Microsoft M365 Multitenant

Workspace and Collaboration Services

NASA Point of Contact: Shane McCaw

Phone Number: 321-210-1660

E-mail: shane.a.mccaw@nasa.gov

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

The National Aeronautics and Space Administration (NASA) Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) NASA collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. NASA publishes its PIAs, as well as its System of Records Notices (SORNs), on the NASA public-facing website, which describes NASA's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

Reviewing Official: Stayce Hoult, Chief Privacy Officer



System Overview: M365 apps may contain PII stored there by users for the purposes of normal day to day work operations, collaboration or simple storage. None of these apps collect that information as part of the processes. Sources may vary widely but are used as a mechanism to store, collaborate and share information between users. The potential PII stored and shared using M365 comes from a varied source of extracts and sources.

1. **Microsoft Office M365-Exchange Online** - Microsoft Office 365-Exchange provides mailbox and calendar functionality while utilizing Software as a Service (SaaS) functionality. NASA end users can access their email "anywhere, anytime" from a variety of clients and platforms.
2. **Office 365 - SharePoint (Online)** - National Aeronautics and Space Administration (NASA) uses the Microsoft Office 365 SharePoint Online to share and manage content, knowledge, and applications to empower teamwork, quickly find information, and seamlessly collaborate across the organization.
3. **Microsoft O365 Teams** - Microsoft Teams is a unified communications platform that combines persistent workplace chat, video meetings, file storage, and application integration. The service integrates with the company's Office 365 subscription office productivity suite and features extensions that can integrate with non-Microsoft products. SharePoint Online and OneDrive are the base storage areas for Teams chats, files and meetings transcripts and recordings.
4. **Microsoft Office 365 - Forms** - Microsoft Forms is an online survey creator, part of Microsoft Office 365. Released by Microsoft in June 2016, Forms allow users to create surveys and quizzes with automatic marking.
5. **Office 365 - Planner** - Microsoft Planner is a simple, light weight Work Management Application that Microsoft is offering as part of their Office 365 subscriptions. Planner lets you organize projects, share files, assign tasks, and chat with other collaborators
6. **Cloud Management Gateway** - The Cloud Management Gateway (CMG) is a Microsoft Azure Cloud Service, Platform as a Service (PaaS), and provides an efficient way to manage System Center Configuration Manager (SCCM) clients over the internet. CMG does not require additional on-premises infrastructure and leverages the existing NASA current infrastructure. CMG will provide OCIO management and patching capabilities without the need for a VPN.
7. **Office 365 Power BI Pro** - O365 Power BI Pro - Power BI is an online software service (SaaS, or Software as a Service) offering from Microsoft that enables users the ability to create self-service Business Intelligence dashboards, reports, datasets, and visualizations. With Power BI, connections are made to different data sources to combine and shape data from those connections, then create reports and dashboards that can be shared with others. The Power BI cloud services work together with Excel to provide a complete self-service analytics solution utilizing excel for authoring reports and Power BI for sharing them. The Power BI service is built on Azure, which is Microsoft's cloud computing platform.
8. **Microsoft Defender for Office 365** - Microsoft Office 365 Advanced Threat Protection (ATP-1) is a cloud-based email filtering service that helps protect the organization

against unknown malware and viruses by providing robust zero-day protection and includes features to safeguard your organization from harmful links in real time. ATP has rich reporting and URL trace capabilities that give administrators insight into the kind of attacks happening in the organization.

9. **Insider Threat and Communication Compliance** - The NASA Insider Threat Program is focused on prevention by taking a proactive approach to deterring, detecting, and mitigating insider threats by analyzing various data sources across NASA for patterns of concerning behavior. A single indicator may say little; however, if taken together with other indicators, a pattern of concerning behavior may arise. The NASA Insider Threat Program coordinates and works closely with the Office of Inspector General, the Office of Protective Services (Security and Counterintelligence), the Office of Chief Information Officer, the Office of Chief Human Capital Officer, the Office of General Counsel, and NASA Privacy Officials.
10. **Microsoft Purview** - a comprehensive set of solutions designed to help organizations govern, protect, and manage data, wherever it lives. It provides integrated coverage to address data fragmentation across organizations, lack of visibility that hampers data protection and governance, and the blurring of traditional IT management roles. Microsoft Purview combines various solutions and services into a unified platform to help organizations gain visibility into their data, safeguard and manage sensitive data across its lifecycle, and govern data seamlessly in new, comprehensive ways.
11. **M365 App Registrations** - app registrations that are included in Azure AD
12. **Microsoft Dataverse** - a cloud-based data storage platform within the Microsoft Power Platform that allows users to store, manage, and access data from various business applications. This will allow Power Automate, Power Apps and Power BI to allow a user to process, display and report (database storage to UI to automation to reporting) entirely hosted in the cloud. This service is under the Microsoft M365 Multitenant license and is governed through the M365 Working Group. Data collected and processed within the Dataverse is through permission from the data owner.

Privacy / Authorities and Other Requirements	
List all legal authorities and/or agreements that permit the collection of privacy information by the project. Explain how these authorities permit the project and the collection of privacy information. If the project collects Social Security numbers, also identify the specific statutory authority allowing it.	EO 14028 Executive Order on Improving the Nation's Cybersecurity NASA-SPEC-2600 Enumeration of ASCS Cybersecurity Requirements NASA-SPEC-2650 Transport Layer Security (TLS) NASA-STD-2601 Minimum Cybersecurity Requirements for Computing Systems NPR 2810.1F Security of Information and Information Systems NPR 2841.1x Identity, Credential, and Access Management 5 USC 552a, OMB Circular A-130, OMB M-03-22, OMB M-07-16, OMB M-10-23, OMB M-99-18,

	PL 100-503, PL 104-191, PL 104-231, PL 107-347, PL 107-347 208, PL 107-347 V, PL 113-187, NARA, FTC, ECFR, NCSL.
The records in the system are covered by an existing published System of Records Notice (SORN).	Existing SORN applicable
The SORN Name and Number.	NASA 10SECR M365 as it is not considered a 'system of records' as defined by the Privacy Act, 5 U.S.C. 552a(a)(5)." Microsoft 365 itself, including its multitenant configuration, is not inherently a system of records. However, if an agency uses M365 to store or retrieve PII in a way that meets the definition of a SOR, then the agency—not Microsoft—must determine whether a SORN is required.

Privacy Act of 1974 / Uses of the Information	
Records on individuals are or will be routinely retrieved from the system by using individual's name or other unique identifier (e.g., personal account number, UUPIC, SSN, etc. is used to locate information about an individual in the application/website/information system/paper record).	Yes

Paperwork Reduction Act / Characterization of the Information	
The record/application/website/information system collects information in a standard way (via forms, surveys, questionnaires, etc.) from 10 or more persons (e.g., members of the public and NASA contractors, and grantees).	Yes

Paperwork Reduction Act / Authorities and Other Requirements	
There is an OMB Control Number.	No
The OMB Control Number.	Each would require its own OMB control number

Privacy / Characterization of the Information	
Information is collected on the following:	NASA Contractors Government Employees

	Members of the public (excluding contractors and partners) Business Partners/Contracts, Grantees (including, but not limited to federal, state, local agencies)
Collection contains the following:	Name Date of birth SSN Vehicle identifier (license plate) Marriage certificate Device identifiers (pacemaker, hearing aid, etc.) Biometric identifier (fingerprint or voiceprint) Employment status and/or records Education records Miscellaneous identification numbers (accounts, permits, etc.) Other PII not listed above Passport number Driver's license number Mother's maiden name Work phone number Work cell phone number Personal cell phone number UUPIC Agency User ID (AUID) Other number originated by a government that specifically identifies an individual Work e-mail address Personal e-mail address School e-mail address Home mailing address Medical records numbers Medical notes X-ray Financial account information Birth certificate Death certificate Legal documents (divorce decree, criminal records, etc.) Military status and/or records Foreign activities and/or interests Photograph Video URL Work Mailing Address Home Phone Number

The collection is the minimum necessary to accomplish the purpose of the collection.	Yes
Discuss the intra-Departmental sharing of information. Identify and list the name(s) of any components or directorates within the Department with which the information is shared.	NASA signed up to use Microsoft Office 365 Multi-tenant to support the Agency's abilities to communicate and collaborate within different organizations and contracts within the Agency. The use of the identifying information allows for proper recipient to receive the correct communication. The system uses Azure Active Directory (AAD) for this purpose.

Privacy / Uses of the Information	
NASA will use the information in the following ways:	M365 is used to communicate and collaborate on various NASA program office projects and activities. The information is used to further their program area missions in an effective and efficient manner that appropriately controls access, provides the ability to track changes and reduce version control issues, and enables appropriate use and sharing of NASA information. M365 services such as Exchange Online allow users to view contact information to interact and work with each other within the collaborative environment and communicate through email and scheduling meetings with internal users and individuals outside NASA.
The application/website/information system stores, collects, or maintains Information in Identifiable Form (IIF).	Yes

Consent / Notice	
Does the project provide individuals notice prior to the collection of information?	Yes
If no, explain why individuals are not notified prior to collection of information.	
If yes, describe how the notice provided for the collection of information is adequate to inform those impacted.	The information included in the system must be supplied by the user to support Office 365's provided functionality. NASA users are provided with training and must sign Rules of Behavior before accessing the system. In addition, they are presented with a NASA Warning Banner prior to logging on to any NASA system, which stipulates users do not have the right to privacy while using the system, which includes internet and email services. Certain applications within Office 365 may provide appropriate notice to individuals whose information may be used or collected within the system. For example, individuals who participate in Teams meetings are provided notice

	if a meeting is going to be recorded. Individuals who provide information to NASA that NASA users may then include in the collaboration components of Office 365 may receive notice at the point of collection regarding the purpose for which that information may be used but not notice of its inclusion in Office 365. This PIA and any relevant SORN also provide notice to individuals.
Do individuals have opportunities to decline to provide information, or opt out of the project?	No
If yes, describe the process. If this is not an option, explain why not.	NASA users and others whose information may be contained in Office 365 generally do not have an opportunity to consent to the inclusion of their information in the system. NASA users cannot decline to provide their information to access Office 365. Individuals who are not NASA users but whose information is contained in the system may have opportunities at the point their information is collected to decline to provide it but once provided cannot decline for it to be included in Office 365. For example, those who participate in Teams meetings receive notice if a meeting is going to be recorded and can opt to leave the meeting or turn off their camera and microphone.
Do individuals have opportunities to consent to specific/targeted uses of their information?	No
If yes, describe the process. If this is not an option, explain why not	The O365 system uses identifiable data for business use only such as email delivery, Teams instant chat and OneDrive storage.
The IIF is collected	Mandatory
There is a process in place for the following:	
Ensuring consent is obtained from the individuals whose IIF is stored, collected, or maintained.	No
Are individuals provided with notice that they have opportunities to consent to uses, decline to provide information, or opt out of the project?	No
If yes, describe the process. If no, explain why not.	NASA users and others whose information may be contained in Office 365 generally do not have an opportunity to consent to the inclusion of their information in the system. NASA users cannot decline to provide their information to access Office 365. Individuals who are not NASA users but whose information is contained in the system may have opportunities at the point their information is collected to decline to provide it but once provided cannot decline for it to be included in Office 365. For example, those who participate in Teams meetings receive notice if a meeting is going to be recorded and can opt to leave the meeting or turn off their camera and microphone.

Are individuals notified of the consequences of providing information?	Yes
If yes, describe the process. If no, explain why not.	The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.

Data Retention	
Explain how long each type of information is retained. Include a justification for the retention period of each information type and how/why that period is necessary to the mission/project.	NASA records are retained in accordance with NASA Records Retention Schedules (NRRS) , which outline the retention periods for various records created and maintained by NASA employees and contractors. These schedules are approved by the National Archives and Records Administration (NARA) and are essential for the proper management and disposition of records. Due to the nature of M365, there may be numerous records schedules with different retention requirements applicable to the records created and maintained by M365 users. It is the responsibility of the respective M365 users to maintain and dispose of the records they create in accordance with the appropriate records retention schedules applicable to their program area

Information Sharing	
Is information shared outside of the organization as part of the normal agency operations?	No
Identify who the information is shared with, how the information is accessed, and how it is to be used.	
Describe how the external sharing noted in the previous question is compatible with the SORN noted in PIA-02.	

Redress	
What are the procedures that allow individuals to access their information?	NASA users have access in the various Office 365 systems to their information. For example, Exchange Online user data can be accessed via Outlook. Others whose information may be contained in an Office 365 application may access their information as appropriate by following the instructions in any applicable system of records notice

What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	Active Directory is an enterprise administrative tool; certain NASA user information hosted in Active Directory is read-only to the individual; a user has access to view the data but can only request appropriate changes and removal by contacting system owners and operators. The Global Address Book is an aspect of Microsoft Outlook; an individual NASA user is encouraged to review their entries in the Global Address List (GAL) to make sure the information is up to date and correct. They can update certain information on NASA's Intranet site or by contacting the NASA Helpdesk to have this information corrected on the GAL. To remove an employee from the GAL, requests must be submitted through the Help Desk. Others whose information is in the system can access and request amendment to their information as appropriate by following the instructions in any applicable system of records notice,
How does the project notify individuals about the procedures for correcting their information?	NASA's Office 365 implementation is not accessible to anyone outside of NASA and, therefore, does not provide notice directly to those individuals who are not NASA users whose information it contains. NASA users receive notice in the form of training, instructions, Rules of Behavior, and the NASA Warning Banner prior to accessing.

Auditing and Accountability	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	The Cloud Service Provider has developed a set of auditable events which incorporates identified vulnerabilities, business requirements, and security standards. Events are audited continually. The NASA SOC monitors O365 activity through the use of Splunk.
Describe what privacy training is provided to users either generally or specifically relevant to the project.	The acceptable Rules of Behavior for NASA data and PII taught through the Saturn course Cybersecurity and Privacy Awareness Training (CPAT). The CPAT course is an annual requirement in accordance with the Federal Information Security Management Act of 2002 (FISMA) and Federal Information Security Modernization Act of 2014 requirement for annual security awareness training for users of federal information systems.
What procedures are in place to determine which users may access the information and how does the project determine who has access?	For all O365 applications, approved authorization for logical access is conducted in NAMS based upon roles provisioned. Additionally, the user must have current Annual Security Training before submitting a NAMS request. This request must indicate to which system(s) the applicant wishes

	to gain access, the access privilege, their department area, and an electronically written justification, along with other pertinent information. O365 is fully integrated with ICAM and NAMS.
How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within the department and outside?	The Information System Owner and Authorizing Official negotiated contracts with Microsoft and authorized the interconnection and flow of information between these systems and services: Microsoft Office 365 Software as a Service; NASA Identity, Credential & Access Management (ICAM); Microsoft Azure Active Directory (AAD); NASA Consolidated Active Directory (NCAD); NASA Access Management System (NAMS); NASA Mobile Device Management (MDM); Microsoft ExpressRoute; NASA Public Key Infrastructure (PKI); Microsoft Threat Defender and NASA's Security Operations Center (SOC). New agreements would follow the same process of requesting access and approval of systems to be allowed access to the O365 Tenant.

Security Controls / Characterization of the Information	
Monitor and Response to privacy and/or security incidents policies.	No

Security Controls / Auditing and Accountability	
Technical controls (safeguards) are in place to minimize the possibility of unauthorized access, use, or dissemination of the IIF in the application/ website/ information system/ cloud system.	Yes
Access controls.	Yes

Information Sharing Practices / Characterization of Information	
The application/website/information system/cloud systems collects IIF from other resources (e.g., databases, websites).	Yes
The application/website/information system/cloud system populates data for other resources (e.g., databases, websites, or external agencies, people, or organizations).	Yes

Accessibility, Redress, Complaints / Characterization of the Information	
There is a process in place for periodic reviews of IIF in the system to ensure data integrity, availability, accuracy, and relevance.	Yes

Web Measurement and Customizing Technology / Characterization of the Information	
The Application/Website/Information System Utilizes Web Measurement and Customization Technology (Cookies/Persistent Tracking).	No

Agency Privacy Manager (APM):

Kostka, Paul A

Midulla, Laura P

Rucker, Anh-Hong N

APM Review Decision: Concur

APM Review Date: 11/26/2025

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 12/10/2025

CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Taylor, Kelvin L

SAISO Review Decision: Concur

SAISO Review Date: 12/10/2025

NASA Senior Agency Official for Privacy (SAOP):

Gallagher, Sean M

SAOP Review Decision: Approve

SAOP Review Date: 12/10/2025

PIA Entry Name: Microsoft Copilot

Worksapce and Collaberation Services

NASA Point of Contact: Shane McCaw

Phone Number: 321-210-1660

E-mail: shane.a.mccaw@nasa.gov

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

The National Aeronautics and Space Administration (NASA) Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) NASA collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. NASA publishes its PIAs, as well as its System of Records Notices (SORNs), on the NASA public-facing website, which describes NASA's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

Reviewing Official: Stayce Hoult, Chief Privacy Officer



System Overview: Microsoft Copilot is an AI-powered digital assistant that aims to provide personalized assistance to users for a range of tasks and activities. Copilot can summarize user's day or week, generate summaries, and analyze contents of documents stored in SharePoint and OneDrive. This will include the M365 productivity apps to include Word, PowerPoint, Excel, OneNote, SharePoint, OneDrive, Teams, and Exchange.

Copilot for M365 is a licensed AI-powered tool for use as a digital assistant. Microsoft 365 Copilot is grounded on users' data, like emails, meetings, and files, data may include PII. Additionally includes Copilot Premium.

Microsoft Copilot Light (M365 Copilot Chat) is a free, limited capability chatbot service. Copilot Chat is AI chat grounded in data from the web and powered by the latest large language models (LLMs). Copilot Chat can't invoke organizational content like files, emails, or chats on its own.

Microsoft Copilot Studio - Copilot Studio is a graphical, low-code tool for building agents and agent flows. It is for use with Power Platform only.

Privacy / Authorities and Other Requirements	
List all legal authorities and/or agreements that permit the collection of privacy information by the project. Explain how these authorities permit the project and the collection of privacy information. If the project collects Social Security numbers, also identify the specific statutory authority allowing it.	Executive. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023) Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence Executive. Order No. 14,179, 90 Fed. Reg. 1125 (Jan. 23, 2025) Removing Barriers to American Leadership in Artificial Intelligence Executive Order 14320, <i>Promoting the Export of the American AI Technology Stack</i>, issued by President Donald J. Trump on July 23, 2025, and published by the White House. Executive Order, Preventing Woke AI in the Federal Government, The White House, July 23, 2025 Office of Mgmt. & Budget, M-25-21 (Apr. 3, 2025) Accelerating Federal Use of AI through Innovation, Governance, and Public Trust Office of Mgmt. & Budget, M-25-22 (Apr. 3, 2025) Driving Efficient Acquisition of Artificial Intelligence in Government

	Office of Mgmt. & Budget, M-24-10 (Mar. 28, 2024) <i>Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence</i> <i>Artificial Intelligence Risk Management Framework (AI RMF 1.0)</i> , NIST AI 100-1 (Jan. 26, 2023) National Institute of Standards and Technology https://doi.org/10.6028/NIST.AI.100-1
The records in the system are covered by an existing published System of Records Notice (SORN).	SORN not required
The SORN Name and Number.	

Privacy Act of 1974 / Uses of the Information	
Records on individuals are or will be routinely retrieved from the system by using individual's name or other unique identifier (e.g., personal account number, UUPIC, SSN, etc. is used to locate information about an individual in the application/website/information system/paper record).	No

Paperwork Reduction Act / Characterization of the Information	
The record/application/website/information system collects information in a standard way (via forms, surveys, questionnaires, etc.) from 10 or more persons (e.g., members of the public and NASA contractors, and grantees).	No

Paperwork Reduction Act / Authorities and Other Requirements	
There is an OMB Control Number.	No
The OMB Control Number.	

Privacy / Characterization of the Information	
Information is collected on the following:	NASA Contractors Government Employees Other
Collection contains the following:	Name Date of birth SSN

	Vehicle identifier (license plate) Marriage certificate Device identifiers (pacemaker, hearing aid, etc.) Biometric identifier (fingerprint or voiceprint) Employment status and/or records Education records Miscellaneous identification numbers (accounts, permits, etc.) Passport number Driver's license number Mother's maiden name Work phone number Personal cell phone number UUPIC Agency User ID (AUID) Other number originated by a government that specifically identifies an individual Work e-mail address Personal e-mail address School e-mail address Home mailing address Medical records numbers Medical notes X-ray Financial account information Birth certificate Death certificate Legal documents (divorce decree, criminal records, etc.) Military status and/or records Foreign activities and/or interests Photograph URL Work Mailing Address Home Phone Number
The collection is the minimum necessary to accomplish the purpose of the collection.	Yes
Discuss the intra-Departmental sharing of information. Identify and list the name(s) of any components or directorates within the Department with which the information is shared.	Upon review and further analysis of data, M365 Copilot output can be shared among various NASA organizations. Information warranting protection will be handled in accordance with NASA's requirements (NPR 2810.7).

Privacy / Uses of the Information

NASA will use the information in the following ways:	Stakeholders will use the information in various ways to communicate and enhance assigned tasks This stored data provides users with Copilot activity history in Microsoft 365 Copilot Chat (previously named Business Chat) and meetings in Microsoft Teams. This data is processed and stored in alignment with contractual commitments with your organization's other content in Microsoft 365. The data is encrypted while it's stored and isn't used to train foundation LLMs, including those used by Microsoft 365 Copilot.
The application/website/information system stores, collects, or maintains Information in Identifiable Form (IIF).	Yes

Consent / Notice	
Does the project provide individuals notice prior to the collection of information?	Yes
If no, explain why individuals are not notified prior to collection of information.	
If yes, describe how the notice provided for the collection of information is adequate to inform those impacted.	[Generally] when information is retrieved, users are notified that the information will be used for the purposes for which it was intended and NASA's Terms of Use are followed.
Do individuals have opportunities to decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If this is not an option, explain why not.	n/a various processes depending on condition for which the data was obtained
Do individuals have opportunities to consent to specific/targeted uses of their information?	No
If yes, describe the process. If this is not an option, explain why not	n/a - we are using the data, not collecting the data. Question not relevant for AI.
The IIF is collected	Voluntary
There is a process in place for the following:	
Ensuring consent is obtained from the individuals whose IIF is stored, collected, or maintained.	Yes
Are individuals provided with notice that they have opportunities to consent to uses, decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If no, explain why not.	n/a - various processes depending on condition for which the data was obtained
Are individuals notified of the consequences of providing information?	Yes

If yes, describe the process. If no, explain why not.	notification and consent provided and obtained considering the circumstance for which the information was collected
---	---

Data Retention	
Explain how long each type of information is retained. Include a justification for the retention period of each information type and how/why that period is necessary to the mission/project.	Copilot interactions are stored in a hidden folder in the users mailbox in Exchange, which are bound to the Exchange retention policies of 7 years.

Information Sharing	
Is information shared outside of the organization as part of the normal agency operations?	No
Identify who the information is shared with, how the information is accessed, and how it is to be used.	n/a
Describe how the external sharing noted in the previous question is compatible with the SORN noted in PIA-02.	

Redress	
What are the procedures that allow individuals to access their information?	n/a Any data protected by the Privacy Act adheres to redress processes outlined in applicable SORN.
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	n/a Any data protected by the Privacy Act adheres to redress processes outlined in applicable SORN.
How does the project notify individuals about the procedures for correcting their information?	n/a Any data protected by the Privacy Act adheres to redress processes outlined in applicable SORN.

Auditing and Accountability	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	NASA follows NIST AI Controls - NASA baseline requirements and NASA critical controls for systems with artificial intelligence (AI) components; CONTROL BASELINES AND CRITICAL CONTROLS FOR NASA INFORMATION SYSTEMS SECURITY CONFIGURATION SPECIFICATION, NASA-SPEC 2661.Controls
Describe what privacy training is provided to users either generally or specifically relevant to the project.	NASA Cybersecurity and Privacy Awareness Training

What procedures are in place to determine which users may access the information and how does the project determine who has access?	AC-02 Account Management AC-03(07) Access Enforcement
How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within the department and outside?	The Authorizing Official (AO) and Information System Owner (ISO) must review Information Sharing Agreements (ISAs).

Security Controls / Characterization of the Information	
Monitor and Response to privacy and/or security incidents policies.	Yes

Security Controls / Auditing and Accountability	
Technical controls (safeguards) are in place to minimize the possibility of unauthorized access, use, or dissemination of the IIF in the application/ website/ information system/ cloud system.	Yes
Access controls.	Yes

Information Sharing Practices / Characterization of Information	
The application/website/information system/cloud systems collects IIF from other resources (e.g., databases, websites).	Yes
The application/website/information system/cloud system populates data for other resources (e.g., databases, websites, or external agencies, people, or organizations).	Yes

Accessibility, Redress, Complaints / Characterization of the Information	
There is a process in place for periodic reviews of IIF in the system to ensure data integrity, availability, accuracy, and relevance.	No

Web Measurement and Customizing Technology / Characterization of the Information	
The Application/Website/Information System Utilizes Web Measurement and Customization Technology (Cookies/Persistent Tracking).	Yes

Agency Privacy Manager (APM):

Kostka, Paul A

Midulla, Laura P

Rucker, Anh-Hong N

APM Review Decision: Concur

APM Review Date: 09/11/2026

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 09/11/2026

CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Taylor, Kelvin L

SAISO Review Decision: Concur

SAISO Review Date: 09/11/2026

NASA Senior Agency Official for Privacy (SAOP):

Gallagher, Sean M

SAOP Review Decision: Approve

SAOP Review Date: 09/11/2026