National Aeronautics and Space Administration

Privacy Impact Assessment (PIA)

PIA Entry Name: Guest Account Services Enterprise Applications Management Office
NASA Point of Contact: Whitney Craig **Phone Number:** 256.682.8876 **E-mail:** whitney.b.craig@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:

Guest.nasa.gov is a web application used by non-NASA identities that need for a NASA Guest account to access public, low-risk web application capabilities supported by NASA.

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.	M-05-24 "Implementation of Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors" M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 Policy for a Common Identification Standard for Federal Employees and Contractors M-16-04 "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" M-04-04 E-Authentication Guidance for Federal Agencies M-19-17 "Enabling Mission Delivery through Improved Identity, Credential and Access Management" NIST 800-63 "Digital Identity Guidelines"
The records in the system are covered by an existing published System of Records Notice (SORN).	Existing SORN applicable
The SORN Name and Number.	The following SORN applies: NASA 10SECR https://www.nasa.gov/privacy/nasa_sorn_10SECR.html

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.	Yes
The OMB Control Number.	OMB-2700-0158

Privacy / Characterization of the Information	
Information is collected on the following:	Members of the public (excluding contractors and partners) Business Partners/Contracts, Grantees (including, but not limited to federal, state, local agencies) Contractors/Vendors/Suppliers
Collection contains the following:	Name Other PII not listed above Personal cell phone number Personal e-mail 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.	Guest.nasa.gov has direct integration with NASA Enterprise Directory (NED). Guest feeds NASA guest identity data into NED.

Privacy / Uses of the Information	
NASA will use the information in the following ways:	Guest identity information is used to vet the guest user to determine Level of Confidence (LoC). For invitational travelers, guest account information is provided to General Service Administration's (GSA) eTravel application to provide payment record.
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.	Any member of the public wishing to request a NASA Guest account must read and acknowledge the NASA Terms of Service which states: By accessing and using this information system, you acknowledge and consent to the following: You are accessing a U.S. Government information system, which includes: (1) this computer; (2) this

	computer network; (3) all computers connected to this network including end user systems; (4) all devices and storage media attached to this network or to any computer on this network; and (5) cloud and remote information services. This information system is provided for U.S. Government-authorized use only. You have no reasonable expectation of privacy regarding any communication transmitted through or data stored on this information system. At any time, and for any lawful purpose, the U.S. Government may monitor, intercept, search, and seize any communication or data transiting, stored on, or traveling to or from this information system. You are NOT authorized to process classified information on this information system. Unauthorized or improper use of this system may result in suspension or loss of access privileges, disciplinary action, and civil and/or criminal penalties.
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.	Members of the public are not required to obtain a NASA Guest account. All NASA guests submit their personally identifiable information voluntarily. If a member of the public chooses not to sign up for a NASA guest account they will not be able to access NASA resources designated for Guest access.
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	NASA guest identities are basic identity records on individuals using minimal identity data. The information is required to vet that the person is who the claim to be and to provide access designated NASA resources.
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.	Users can update information under Guest.nasa.gov and can terminate their accounts. Guest users accounts are deleted if an account closure request is submitted.
Are individuals notified of the consequences of providing information?	Yes

If yes, describe the process. If no, explain why not.	Per the Terms of Service "By access and using this information system, you acknowledge and consent - You have no reasonable expectation of privacy regarding any communication transmitted through or data stored on this information system. At any time, and for any lawful purpose, the U.S. Government may monitor, intercept, search, and seize any communication or data transiting, stored on, or traveling to or from this information system. "

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.	There is no NASA Records of Retention Schedule (NRRS) for Guest identities. Guest data is a very low risk, the record is deleted after the lifetime of that Guest account. Guest identities only have access for 60 days, an extension can be extended up to a maximum of 1 year, and the Guest user much change their password every 60 days. Following the 60 days to 1 years maximum the account is disabled and the data for that account deleted. NASA does not maintain a records history.

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?	User must identify and authenticate using NASA login credentials or "Log in Google," however limited identity data can be updated via Guest.nasa.gov
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	Users submit their own information, Self-Managed users will go to https://guest.nasa.gov to create and manage their accounts.

How does the project notify individuals about the procedures for correcting their information?	Users submit their own information. Individuals are able to update limited PII elements using https://guest.nasa.gov.

Auditing and Accountability	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	There is an annual Certificate & Accreditation (C&A) where all National Institute of Standards and Technology (NIST) 800-53 controls are investigated and validated. All audit logs from Guest are recorded and maintained for the length of time per NASA policy stated in ITS-HBK-2810.16-01. NASA Access Management System (NAMS) tracks all user access requests and are validated annually.
Describe what privacy training is provided to users either generally or specifically relevant to the project.	No training is provided to Guest Account users because this is targeted for members of the public who are not required to take privacy training. System Administrators and NASA personnel are required to take security and privacy training annually, as well as applicable role-based training.
What procedures are in place to determine which users may access the information and how does the project determine who has access?	A unique email address that is not identified by any other existing NASA identity is used to determine who has access.
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?	Memorandum of Understanding (MOU) and Interconnection Service Agreements (ISA) are notated within the System Security Plan. These are reviewed and approved per the maintenance lifecycle.

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.	Yes

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):

Guerin, Michael D
HARRIS HOULT, STAYCE D
Kostka, Paul A
Midulla, Laura P
Montasser, Ali S
Scholz, Matthew C
zzzINACTIVE20250402 - Hill, Debra A

APM Review Decision: Concur

APM Review Date: 07/15/2024

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 11/14/2024

STAYCE HARRIS HOULT Digitally signed by STAYCE HARRIS HOULT
Date: 2025.05.14 09:47:17 -05'00'

CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Witt, Michael

SAISO Review Decision: Concur

SAISO Review Date: 12/04/2024

NASA Senior Agency Official for Privacy (SAOP):

SEATON, JEFFREY M

SAOP Review Decision: Approve

SAOP Review Date: 04/08/2025