National Aeronautics and Space Administration

Privacy Impact Assessment (PIA)

PIA Entry Name: Personal Identity Verification Issuance (BMS, BioSP, CMS)

Enterprise Applications Management Office

NASA Point of Contact: Nichole Benson

Phone Number: 256.542.8867

E-mail: nichole.m.benson@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:

PIV Issuance is comprised of three applications which support the various stages of issuing PIV badges to users.

Card Management System (CMS) is a COTS application delivered by Active Identity. CMS is the application that manages PIV credentials for production, termination, encoding and finalization. It is used to store the identities of cardholders provisioned through Identity Management and Account Exchange (IdMAX). Software located on the issuance workstation allows the issuance official to access the provisioned identities in order to encode and finalize badges.

Batch Management System (BMS) is used to place PIV card orders to the vendor, Oberthur. BMS is the application that merges card production requests into a single job that is submitted to a card production service.

Biometric Application Server (BioSP) is accessed via the Universal Registration Client (URC) to capture enrollment details. BioSP is the storage service for identity biometrics; I9, fingerprints, signature, physical attributes, badge photograph.

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-19-17 "Enabling Mission Delivery through Improved Identity, Credential, and Access Management" M-16-04 "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" 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-04-04 E-Authentication Guidance for Federal Agencies OMB 2700-0158 Personal Identity Validation for Routine and Intermittent Access to NASA Facilities, Sites and Information Systems E-Gov Act of 2002 applies in section 208 PLAW-107publ347.pdf (govinfo.gov)
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).	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 Business Partners/Contracts, Grantees (including, but not limited to federal, state, local agencies) Contractors/Vendors/Suppliers
Collection contains the following:	Name Date of birth SSN Biometric identifier (fingerprint or voiceprint) Other PII not listed above Passport number Driver's license number UUPIC Agency User ID (AUID) Work e-mail address Birth certificate Legal documents (divorce decree, criminal records, etc.) Photograph
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.	There is no intra-departmental sharing of information coming from or to PIV Issuance applications.

Privacy / Uses of the Information	
NASA will use the information in the following ways:	PIV Issuance applications use identity information in order to create an identity record. Although the identity record is used primarily to gain access into NASA systems, these records may be disclosed to: 1. To the Department of Justice when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records. 2. To a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records. 3. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained. 4. To a staff member of the Executive Office of the President in response to an inquiry from the White House.

	5. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. §§ 2904 and 2906. 6. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a. 7. To any official investigative or judicial source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested. 8. To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy, consistent with Freedom of Information Act standards. 9. To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives. 10. To notify another Federal agency when, or verify whether, a PIV card is no longer valid. 11. Disclosure to a NASA contractor, subcontractor, grantee, or other Government organization information developed in an investigation or administrative inquiry concerning a violation of a Federal or state statute or

	regulation on the part of an officer or employee of the contractor, subcontractor, grantee, or other Government organization. 12. NASA standard routine uses as set forth in Appendix B.
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.	CMS and BMS inherit their notices from Identity Management and Account Exchange (IdMAX) . For BioSP the Public Key Infrastructure (PKI) Terms of Service must be acknowledged by the enrollee during the enrollment process.
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.	Any NASA identity who declines to provide information or opt out will not be able obtain a Personal Identity Verification (PIV) card or credential.
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	Creating a NASA Identity means generating a record in the Identity Workflow that establishes a relationship between the applicant and NASA. Individuals are responsible for completing all required fields, which is used to establish a Level of Confidence for an identity. The IdMAX User Handbook and ICAM Handbook IT-HBK 2841-003A provide further insight into the described process.
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?	No

If yes, describe the process. If no, explain why not.	Federal employees and contractors who access NASA network and systems must agree to the collection of information for background investigation in order to gain logical access to NASA data and physical access to NASA facilities. If an individual refuses to provide the appropriate information, they refuse access to NASA resources and data. Prior to providing identity information all users must read and acknowledge the NASA Terms of Service in accordance with the ITS-HBK 2841-03A ICAM Handbook and NPR 2841.1.
Are individuals notified of the consequences of providing information?	No
If yes, describe the process. If no, explain why not.	This is an inherited process from Identity Management and Account Exchange (IdMAX) which states: AUTHORITY: 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended PURPOSE: To collect information from persons requesting access to NASA assets and/or resources in order to establish an identity and determine eligibility for access. ROUTINE USES: Use and disclosure of your records within and outside of NASA may occur in accordance with the NASA Security Records System Privacy Act System of Record Notices published at https://www.nasa.gov/content/nasa-privacy-act-system-of-records-notices-sorns and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)). DISCLOSURE: Providing this information is voluntary; however, failure to provide the requested information may result in the denial of access."

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.	Per the *NRRS 1441.1* The NASA Records Retention Schedule and *SORN 10SECR,* Personnel Security Records are maintained in Agency files and destroyed upon notification of the death or within 5 years after separation or transfer of employee or within 5 years after contract relationship expires, whichever is applicable in accordance with NASA Records Retention Schedules (NRRS), Schedule 1 Item 103. Personnel Security Records are compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access

	to classified information have been exempted by the Administrator under 5 U.S.C. 552a(k)(5) from the access provisions of the Act. The Personal Identity Records are maintained in Agency files and destroyed upon notification of the death or within 5 years after separation or transfer of employee or within 5 years after contract relationship expires, whichever is applicable in accordance with NRRS, Schedule 1 Item 103. Visitor files are maintained and destroyed in accordance with NRRS, Schedule 1 Item 114. Personal Identity Records are compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information have been exempted by the Administrator under 5 U.S.C. 552a(k)(5) from the access provisions of the Act. The Emergency Data Records are maintained in Agency files and destroyed when superseded or obsolete in accordance with NRRS 1, Item 100B. Emergency Data Records are compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information have been exempted by the Administrator under 5 U.S.C. 552a(k)(5) from the access provisions of the Act. The Criminal Matter Records are maintained in Agency files and destroyed in accordance with Items A and B of National Archives and Records Administration Disposition Authorization N1-255-07-2 after its approval by the Archivist of the United States. Criminal Matter Records are compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information have been exempted by the Administrator under 5 U.S.C. 552a(k)(5) from the access provisions of the Act. The Traffic Management Records are maintained in Agency files and destroyed in accordance with Item C of National Archives and Records Administration Disposition Authorization N1-255-07-2 after its approval by the Archivist of the United States. Traffic Management Records may be obtained from the cognizant system or subsystem manager listed above. Requests must contain the following identifying data concerning the requestor: First, middle, and last name; date of birth; Social Security Number; period and place of employment with NASA, if applicable.

Information Sharing	
Is information shared outside of the organization as part of the normal agency operations?	Yes
Identify who the information is shared with, how the information is accessed, and how it is to be used.	Idemia uses select NASA identity attributes in order to print the users Personal Identity Verification card. Finger print information is provided to Federal Bureau of Investigations (FBI)
Describe how the external sharing noted in the previous question is compatible with the SORN noted in PIA-02.	Per SORN 10SECR "To provide relevant information to an internal or external organization or element thereof conducting audit activities of a NASA contractor or subcontractor." **Record Source Categories**: Information is obtained from a variety of sources including the employee, contractor, or applicant via use of the Standard Form (SF) SF–85, SF–85P, or SF–86 and personal interviews; employers' and former employers' records; FBI criminal history records and other databases; financial institutions and credit reports; medical records and health care providers; educational institutions; interviews of witnesses such as neighbors, friends, coworkers, business associates, teachers, landlords, or family members; tax records; and other public records. Security violation information is obtained from a variety of sources, such as guard reports, security inspections, witnesses, supervisor's reports, audit reports.

Redress	
What are the procedures that allow individuals to access their information?	NASA enrollees cannot access their personally identifiable information in PIV Issuance applications.
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	NASA enrollees cannot access their personally identifiable information in PIV Issuance applications. If updates are required on the enrollee, a new enrollment would have to be initiated.
How does the project notify individuals about the procedures for correcting their information?	There is no notification to individuals about procedures for correcting information.

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) on PIV Issuance where all National Institute of Standards and Technology (NIST) 800-53 controls are investigated and validated. All audit logs from PIV Issuance applications 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.	Role holders have specific training required by NASA. New employees must take Introduction to Information Technology Security and Privacy Awareness for New Employees. All NASA users are required to take an annual Cyber security and Sensitive Unclassified Information Awareness Training and acknowledge the Rules of Behavior.
What procedures are in place to determine which users may access the information and how does the project determine who has access?	The NASA Access Management System, controls the workflow approval and provisioning of user 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).	No

Agency Privacy Manager (APM):

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

APM Review Decision: Concur

APM Review Date: 03/23/2022

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 07/21/2022

STAYCE HARRIS HOULT

Digitally signed by STAYCE HARRIS HOULT
Date: 2025.03.24 15:52:19 -05'00'

CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Witt, Michael

SAISO Review Decision: Concur

SAISO Review Date: 10/24/2022

NASA Senior Agency Official for Privacy (SAOP):

SEATON, JEFFREY M

SAOP Review Decision: Approve

SAOP Review Date: 02/16/2023