National Aeronautics and Space Administration

Privacy Impact Assessment (PIA)

PIA Entry Name: National Center for Critical Information Processing and Storage (NCCIPS) Facility Operation System (FOPS) Privacy Impact Assessment

NASA Shared Services Center

NASA Point of Contact: Robert Poncet

Phone Number: 228-813-3990

E-mail: robert.a.poncet@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:

The NCCIPS FOPS System provides Controlled Unclassified Information (CUI) network services on an isolated network including camera systems, building security, Voice over IP, electrical monitoring of Supervisory Control and Data Acquisition (SCADA) devices, building automations, and inventory network control using specialized computer applications. NCCIPS FOPS encompasses a variety of engineering and administrative applications, some on single-use platforms.

This PIA will Cover One software application on the FOPS Information System.

1. Centralized Control of User and Reader Environment - (**CCURE**) Badging Access

The CCURE application is a badging software application that houses employee's pictures. This allows access control to know who is badging in and out of each area of the facility.

The National Center for Critical Information Processing and Storage (NCCIPS) provides colocated data center facility infrastructure operations, maintenance, project management, and overall facilities management expertise in support of multiple Federal Agencies which are NCCIPS Customers. Our air gapped Facility Operation System (FOPS) network supports a variety of industrial, technical, administrative, business, and security requirements. These include but are not limited to Access Control, Security Camera System Monitoring, building automation systems, and warehouse inventory management using specialized computer applications. As such, services provided require the collection and retention of Personal Identifiable Information (PII) in accordance with processing requirements and legal compliance with federal laws. These include but are not limited to NPR 1600.1A NASA Procedural Requirements, 2.1 Security Controls at NASA Centers:

a. Validate the personnel identification and access eligibility of all personnel entering NASA property by visually examining Federal identification or locally produced, temporary visitor identification or passes.
b. Visually match the photograph with the face of the person presenting the identification.
c. Authenticate identification cards and access using automated means where available.

Specifically, an individual's name and facial photograph are collected and retained for NCCIPS Access Control using the CCURE application. No other PII is collected or retained. Name and facial photograph are collected and retained for the following types of personnel: Government Employees, NASA Contractors, Business Partners/Contracts, Contractors, Vendors, and Suppliers. CCURE enables security managers to create processes and policies to provision, manage, and revoke physical security access privileges for NCCIPS facilities.

During the enrollment workflow, all personnel are provided a Privacy Notice identifying the collection and retention of name and facial photograph. Any personnel who decline to provide the required information or who opt out will not be provided an access card and will be denied access to NCCIPS facilities.

NCCIPS maintains strict governance policies and management for all privacy information collected and retained according to policy mandated by procedural requirements documented in the following: NASA Policy Directive (NPD) 1382.17K – NASA Privacy Policy.

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.	Authorities include: • 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”
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 SORN 10 SECR - CM

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 Other
Collection contains the following:	Name Work phone number Work cell phone number Personal cell phone number 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.	N/A

Privacy / Uses of the Information	
NASA will use the information in the following ways:	For granting and monitoring badge access to the National Center for Critical Information Processing and Storage (NCCIPS) facility
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.	Individuals are notified as the information is being collected.

If yes, describe how the notice provided for the collection of information is adequate to inform those impacted.	This information is being collected and aligned to an individual's Personal Identity Verification Management (PIV) card to access the NCCIPS facilities; to ensure the safety and security of the NCCIPS facilities, systems, and information, and our occupants and users; and verify that all persons entering NCCIPS facilities, using federal information resources, are authorized to do so.
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.	If an individual declines to provide requested information, they will not be granted badge access to the facility.
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 mission does not use the information for specific/targeted use.
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.	Badging access (Name / Photo) from PIV card is required in order to work at the NCCIPS facility. If an individual declines to provide requested information, they will not be granted badge access to the facility.
Are individuals notified of the consequences of providing information?	Yes
If yes, describe the process. If no, explain why not.	Badging access (Name / Photo) from PIV card is required in order to work at the National Center for Critical Information Processing and Storage (NCCIPS) Facility Operation System (FOPS) If an individual declines to provide requested information, they will not be granted badge access to the facility.

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.	Pictures of employees / contractors are retained for the life of employment with NCCIPS plus 6 years per General Records Schedule (GRS) 5.6-120.

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?	See NASA SORN 10 SECR
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	See NASA SORN 10 SECR
How does the project notify individuals about the procedures for correcting their information?	See NASA SORN 10 SECR

Auditing and Accountability	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	The Centralized Control of User and Reader Environment (CCURE) System has read only access. The access and information within the application is only accessible by Access control. Access control is located within the NCCIPS facility behind a locked door that requires badging access. The information is used in accordance with NASA/ NIST Privacy controls.
Describe what privacy training is provided to users either generally or specifically relevant to the project.	Annual IT Security awareness training.
What procedures are in place to determine which users may access the information and how does the project determine who has access?	Access Control and physical security are the only departments that have access to the information (Name, Picture).
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 FOPS system is an air gapped system. The information system does not share information.

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).	No
The application/website/information system/cloud system populates data for other resources (e.g., databases, websites, or external agencies, people, or organizations).	No

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
Kostka, Paul A
Midulla, Laura P
Montasser, Ali S
Scholz, Matthew C

APM Review Decision: Concur

APM Review Date: 11/15/2023

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 03/03/2025

STAYCE HARRIS HOULT

Digitally signed by STAYCE HARRIS HOULT
Date: 2025.05.14 10:21:11 -05'00'

CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Witt, Michael

SAISO Review Decision: Concur

SAISO Review Date: 03/14/2025

NASA Senior Agency Official for Privacy (SAOP):

SEATON, JEFFREY M

SAOP Review Decision: Approve

SAOP Review Date: 04/08/2025