



## Privacy Impact Assessment (PIA)

**PIA Entry Name:** ARC Protective Services Office (PSO) Records Management System (RMS, dispatch)

IT Operations Division

**NASA Point of Contact:** George Reyes

**Phone Number:** 650.604.4344

**E-mail:** george.reyes-1@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:**

Database containing logs of officer interactions and common tasks, including traffic violations and other on site call outs.

<b>Privacy / Authorities and Other Requirements</b>	
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.	<p>Federal Regulations on Privacy and Civil Liberties and the Information Sharing Environment Criminal Justice Information Systems, 28 CFR Part 20 – This regulation is in three sections: Subpart A (General Provisions related to purpose and authority, and providing pertinent definitions); Subpart B (related to state and local criminal history information systems); and Subpart C (related to Federal systems and exchange of criminal history record information).</p> <p>Authority for this activity is derived from: 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended; Espionage and Information Control Statutes, 18 U.S.C. 793-799; Sabotage Statutes, 18 U.S.C. 2151--2157; Conspiracy Statute, 18 U.S.C. 371; 18 U.S.C. 202-208, 3056; Internal Security Act of 1950; Atomic Energy Act of 1954, as amended; Executive Order 12958, as amended, Classified National Security Information; Executive Order 12968, as amended, Access to Classified Information; Executive Order 10865, Safeguarding Classified Information Within Industry; Executive Order 10450, Security Requirements for Government Employees; Pub. L. 81-733; 5 U.S.C. 552a,</p>
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 10 SECR

<b>Privacy Act of 1974 / Uses of the Information</b>	
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

<b>Paperwork Reduction Act / Characterization of the Information</b>
--

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.	

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) Contractors/Vendors/Suppliers
Collection contains the following:	Name Date of birth Driver's license number Work phone number Work cell phone number Personal cell phone number 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.	PII/IIF data is not shared between departments

Privacy / Uses of the Information	
NASA will use the information in the following ways:	If the person has multiple infractions, then the person could lose the privileges pertaining to those infractions.  Emergency personnel (medical/fire) may use the information during an emergency.
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.	The officer gives verbal notice
If yes, describe how the notice provided for the collection of information is adequate to inform those impacted.	
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 they decline, the consequences depend on the infraction
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
The IIF is collected	Voluntary
<b>There is a process in place for the following:</b>	
Ensuring consent is obtained from the individuals whose IIF is stored, collected, or maintained.	Not Applicable
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.	The person can refuse to provide the information to the Officer
Are individuals notified of the consequences of providing information?	Yes
If yes, describe the process. If no, explain why not.	The data is not used again unless there is another infraction

<b>Data Retention</b>	
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.	Information is retained indefinitely. This is in accordance with Law Enforcement requirements and NASA record retention policies.

<b>Information Sharing</b>	
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.	
---	--

<b>Redress</b>	
What are the procedures that allow individuals to access their information?	Individuals may access data in accordance with the Privacy Act see NASA 10 SECR
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	Individuals may access data in accordance with the Privacy Act see NASA 10 SECR
How does the project notify individuals about the procedures for correcting their information?	Individuals may access data in accordance with the Privacy Act see NASA 10 SECR

<b>Auditing and Accountability</b>	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	The authorized personnel with access to the database, are trained to ensure the data is only used in the method described by Law Enforcement policies
Describe what privacy training is provided to users either generally or specifically relevant to the project.	Yearly SATERN Cybersecurity and Privacy Awareness Training (CPAT). All those with access also take an annual web-based re-certification course provided by the Santa Clara County Sheriff's Office
What procedures are in place to determine which users may access the information and how does the project determine who has access?	Requests are made via IdMAX, approvals are via the workflow associated with the request. Approval/Denial is based on requestor's position designation
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?	N/A - The information is not shared outside Protective Services

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

<b>Security Controls / Auditing and Accountability</b>	
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

<b>Information Sharing Practices / Characterization of Information</b>	
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

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

<b>Web Measurement and Customizing Technology / Characterization of the Information</b>	
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

**APM Review Decision:** Concur

**APM Review Date:** 10/18/2022

**Chief Privacy Officer (CPO):**

HARRIS HOULT, STAYCE D

**CPO Review Decision:** Concur

**CPO Review Date:** 10/09/2024

---

CPO Digital Signature

**NASA Senior Agency Information Security Officer (SAISO):**

Witt, Michael

**SAISO Review Decision:** Concur

**SAISO Review Date:** 10/21/2024

**NASA Senior Agency Official for Privacy (SAOP):**

SEATON, JEFFREY M

**SAOP Review Decision:** Approve

**SAOP Review Date:** 04/08/2025