



## Privacy Impact Assessment (PIA)

<p><b>PIA Entry Name:</b> Deep Space Network Operation Support Jet Propulsion Laboratory</p>
<p><b>NASA Point of Contact:</b></p> <p><b>Phone Number:</b></p> <p><b>E-mail:</b></p>
<p><b>PURPOSE OF THE PRIVACY IMPACT ASSESSMENT</b></p> <p>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.</p>
<p><b>Reviewing Official:</b> Stayce Hoult, Chief Privacy Officer</p>



## System Overview:

### Initial Privacy Impact Assessment For DSN Operation Support

Privacy / Authorities and Other Requirements	
<p>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>	<p>Madrid Deep Space Communications Complex (MDSCC) is following the NASA NPR 1620.3B Physical Security Requirements for NASA Facilities and Property requirements to verify contractor and visitor information as well as implement video surveillance. Video is considered PII. Below is the exact verbiage from the NPR that requires DSN to implement video surveillance.</p> <p>NPR 1620.3B Table F</p> <p>Provide video coverage of screening checkpoints, pedestrian and vehicle entrances, exits, loading docks, lobbies, facility perimeter, parking areas, sensitive interior areas, and other potential access points.</p> <p>NPR 1620.3B Table L</p> <p>Certain facilities or VMS views shall be actively monitored (including using alarm/IDS integrated VMS cameras) to facilitate real-time detection and investigation of an incident and to coordinate an active response to an incident. Other facilities or views may be recorded for forensic purposes only. Security personnel assigned to actively monitor VMS should be relieved regularly and only be tasked to monitor a limited number of camera views to alleviate fatigue and inattentiveness. Security officials should determine the length of time that personnel can effectively monitor cameras based on the number of views and other activities. An option to minimize fatigue and maximize coverage is the use of sequencing and</p> <p>VMS Monitoring and multiplexing of multiple camera views on the same screen.</p> <p>Recording</p> <p>VMS recording is intended to develop and maintain a video log of activities which may be referenced if an event is noted after the fact.</p> <p>The minimum length of time for which digital images will be stored is 30 days. CCPS/CCS should establish protocols to minimize and control access to the VMS operating system and stored images.</p> <p>Considerations for VMS monitoring, recording, and storage include:</p> <ul style="list-style-type: none"><li>- If the VMS data is to be transmitted on an IT LAN, determine if the LAN has the capability of</li></ul>

	providing the minimum level of video resolution, frame rate, and system reliability to satisfy physical security protection needs.
The records in the system are covered by an existing published System of Records Notice (SORN).	SORN not required
The SORN Name and Number.	

<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).	No

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

<b>Privacy / Characterization of the Information</b>	
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 Vehicle identifier (license plate) Employment status and/or records Passport number Work e-mail address Video
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 there is no intra-Departmental sharing of data
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------

<b>Privacy / Uses of the Information</b>	
NASA will use the information in the following ways:	Security may use the information to support investigations if an incident occurred and they need to know who was present at the time.
The application/website/information system stores, collects, or maintains Information in Identifiable Form (IIF).	Yes

<b>Consent / Notice</b>	
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.	For the video surveillance there is notifications clearly posted at ingress/egress points to make everyone aware they are being recorded in accordance with GDPR.
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.	Individuals do not have to give their information. They have the right to leave the premises.
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 collections are based on legitimate business needs to support after the fact investigations. Individuals do not have the ability to consent to this targeted use of their information. However, they do have the right to refuse entry so as to avoid being recorded on video, and they have the right to be forgotten by emailing ISDEFE at <a href="mailto:protecciondatos@isdefe.es">protecciondatos@isdefe.es</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.	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.	For the video surveillance there is notifications clearly posted at ingress/egress points to make

	everyone aware they are being recorded. Security officers also verbally ask for permission prior to receiving individuals passports for individuals verification.
Are individuals notified of the consequences of providing information?	Yes
If yes, describe the process. If no, explain why not.	For video surveillance, posted signs explain that video is obtained for security purposes. For collection of passports, security explains this is for verification of individuals entering 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.	The data for the video surveillance and the visitor logs are kept for 30 days. This is necessary to help support after the fact investigations.
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------

### 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?	Visitors have the right to look at their data, update their data, or have their data removed (be forgotten). They have to write to ISDEFE and submit a letter or email to <a href="mailto:protecciondatos@isdefe.es">protecciondatos@isdefe.es</a>
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	Visitors have the right to look at their data, update their data, or have their data removed. They have to write to ISDEFE and submit a letter or email to <a href="mailto:protecciondatos@isdefe.es">protecciondatos@isdefe.es</a>
How does the project notify individuals about the procedures for correcting their information?	The notice is posted at the main gate at the entrance of the complex. Additionally, individuals can request this information after they leave the facility by contacting MDSCC security via email or phone and the information would be provided.

### Auditing and Accountability

How does the project ensure that the information is used in accordance with stated practices in this PIA?	The employees who handle the information is MDSCC security and they are trained not to share the information without authorization from NASA. MDSCC security is also trained to comply with NASA NPR 1620.3B Physical Security Requirements for NASA Facilities and Property.
Describe what privacy training is provided to users either generally or specifically relevant to the project.	Training from Satern, as well as JPL and ISEDEFE, all conduct security and privacy training annually. MDSCC security also trains the security officers collecting the information not to share the data outside the organization.
What procedures are in place to determine which users may access the information and how does the project determine who has access?	Only MDSCC security staff are authorized to see the data. And no data sharing is allowed other than to support investigations for NASA.
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?	No data sharing is allowed other than to support investigations for NASA.

### **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
----------------------------------------------------------------------------------------------------------------------------------------	-----

<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).	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:** 03/06/2024

**Chief Privacy Officer (CPO):**

HARRIS HOULT, STAYCE D

**CPO Review Decision:** Concur

**CPO Review Date:** 03/21/2025

---

CPO Digital Signature

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

Witt, Michael

**SAISO Review Decision:** Concur

**SAISO Review Date:** 03/24/2025

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

SEATON, JEFFREY M

**SAOP Review Decision:** Approve

**SAOP Review Date:** 03/31/2025