National Aeronautics and Space Administration

Privacy Impact Assessment (PIA)

PIA Entry Name: ReadyOp

Protective Services

NASA Point of Contact: Johnson, Jeffery T

Phone Number: 281.483.9778

E-mail: jeffery.t.johnson@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 ReadyOP SaaS is a secure, web-based communication tool designed to serve as a comprehensive emergency management solution at the Johnson Space Center (JSC). It facilitates rapid, interoperable communication through various channels, including email, text, file sharing, rosters, emergency plans, and radio recordings. This tool is accessible via desktops, laptops, and other IP-enabled devices. In the event of an emergency at JSC, the Center Operations Directorate will utilize the ReadyOp platform to communicate with first responders, the emergency response team, and all levels of management. Hosted on Amazon Web Services (AWS) GovCloud and in the FedRAMP certification process at the Moderate level, ReadyOp allows JSC to integrate critical communication platforms. As part of the JSC network, ReadyOp uses a secure direct internet or wireless connection, with features that work both onsite and offsite.

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.	ReadyOp is designed to support JSC Emergency Management Plan activities and aligns with the National Response Framework and the National Incident Management System, ensuring effective incident and emergency planning through immediate information access and fast, flexible communication. In addition, NPR 8715.2B NASA Emergency Management Program Procedural Requirements and NPR 1600.1A NASA Security Program Procedural Requirements are associated with this project.
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 10SECR: Security Records System

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
Collection contains the following:	Name Work phone number Work cell phone number Personal cell phone number UUPIC Work e-mail address 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.	Limited role-based intra-departmental sharing of the information. Information is shared internally within JSC among authorized emergency response and recovery teams (e.g., Protective Services, ride-out teams) strictly for operational purposes and under NAMS-approved access controls

Privacy / Uses of the Information	
NASA will use the information in the following ways:	To dispatch and communicate with first responders, the emergency response team, and provide damage information to recovery teams
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.	Operationally, responding officers provide notice verbally when collecting directly from an individual. ReadyOp system maintains a publicly-visible Privacy Policy and Terms of Use, which all users agree to by using the platform, regarding

	requirements for system use and access. See: Terms of Use | ReadyOp, https://www.readyop.com/terms-of-use/. https://www.readyop.com/privacy-policy/
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.	Consent pertains to operational use within NASA. If they decline, the consequences depend on the situation or infraction. Officers may not be able to assist individuals or provide access to Agency centers or facilities.
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	Federal employees and contractors are required to have user identity in NED. If an individual refuses to provide the appropriate information, they refuse access to NASA networks, systems and data.
The IIF is collected	Mandatory
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.	Consent is implied by volunteering to provide information. By doing so, you are giving NASA your permission to use the information for the intended purpose.
Are individuals notified of the consequences of providing information?	No
If yes, describe the process. If no, explain why not.	Federal employees and contractors who access NASA network and systems are required to have NASA user identity in NED. If an individual refuses to provide the appropriate information, they refuse access to NASA networks, systems and data. Prior to providing identity information all users must read and acknowledge the NASA Terms of Service. For JSC specifically there will inability to grant access and provide assistance.

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.	Data retention is in accordance with NASA policy. NRRS 1441 01/097.5.C PROTECTIVE SERVICE INCIDENT RECORDS, 01/100.0.B SECURITY OPERATIONS

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?	Individuals would have to contact JSC Protective Services for any discrepancies in the information they provided during an incident.
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	In the event that individuals have found inaccuracies in their collected data, they can have it updated with the individuals at protective services at Johnson Space enter. The ReadyOp Agency administrator can request limited updated information from individuals (new users, new recovery/tactical team members) via an email link to a web form allowing them to update their information.
How does the project notify individuals about the procedures for correcting their information?	Information can be provided during the call placed by the individual, or upon contacting JSC Protective Services, or it is made available during a incident in which a report is created. The ReadyOp Agency administrator can request limited information updates from individuals via an email link to a web form allowing them to update their information.

Auditing and Accountability	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	ReadyOp has procured the services of a FedRAMP monitoring firm to to ensure ongoing compliance, thereby facilitating an annual Third-Party Assessment Organization (3PAO) evaluation. NASA will review the evaluation results annually to ensure stated practices are maintained. In addition, NASA stakeholders meet regularly with the ReadyOp representatives.
Describe what privacy training is provided to users either generally or specifically relevant to the project.	Annual Cybersecurity and Privacy Awareness Training and SATERN 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?	ICAM is integrated with ReadyOP SaaS as NASA utilizes the PIV/Smartcard authentication method SAML 2.0. For mobile application access the

	Microsoft Intune derived PIV credential is employed. Approved NAMS requests establish access permissions for the ReadyOp website, specifying the authorized level of interaction for each individual. Login activities are logged and can be restricted or revoked at any time. There is a manual log review process in place.
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?	ReadyOp does share information externally. NAMS is in place to initiate new access to the system by organizations within the department

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).	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.	Not Applicable

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):

Kostka, Paul A
Midulla, Laura P
Rucker, Anh-Hong N

APM Review Decision: Concur

APM Review Date: 05/13/2026

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 05/26/2026

_____
CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Taylor, Kelvin L

SAISO Review Decision: Concur

SAISO Review Date: 06/05/2026

NASA Senior Agency Official for Privacy (SAOP):

Gallagher, Sean M

SAOP Review Decision: Approve

SAOP Review Date: 06/10/2026