Privacy Impact Assessment (PIA): OS - ASPR Ready - QTR2 - 2021 - OS1084401

Date Signed: 7/12/2021

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1340768
PIA Name:	OS - ASPR Ready - QTR2 - 2021 - OS1084401	**Title:**	OS - HHS Assistant Secretary for Preparedness and Response Ready
OpDiv:	OS		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Implementation
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	Yes

URL Details

Type of URL	List Of URL
Publicly accessible website with log in	asprready.hhs.gov

PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	7/1/2021
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	United States Department of Health and Human Services (HHS) Assistant Secretary for Preparedness and Response (ASPR) Ready is a

		system that streamlines agency collaboration, information and data management, and provides the Common Operating Picture for ASPR's preparedness and response missions. The initial ASPR Ready release will include the Information Requests module that allows users to submit questions and receive responses from subject matter experts. The preparedness and data response management includes resource requests (e.g., responders, supplies, equipment) for disasters and planned events (e.g., Presidential Inauguration, State of the Union address). These activities involve managing these requests, tracking resources until they arrive at their destination site. The Common Operating Picture displays a graphical representation of the resources deployed (e.g., responders, supplies, equipment), where the resources are deployed, and the associated event (e.g., hurricanes, wildfires, planned events.) During these events, other agencies, entities, state and local jurisdictions may request information related to these responses (e.g., how many personnel were deployed for Hurricane Laura). Requests may come from other divisions within ASPR, United States Department of Defense (DoD), Centers for Disease Control Prevention (CDC), United States Department of Homeland Security (DHS), states, and local jurisdictions. Additional requests may come from non-government entities including the media. No PII data is exchanged for these responses. The system collects the requested information and the responses to the requests.
PTA -9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	ASPR Ready collects information related to Information Requests. Data elements include: requestor name, requestor phone number, requestor email address, requesting organization, state, situation, subject, summary of request, request on behalf of name, request on behalf of phone number, request on behalf of email, due date, request priority, request status, assignee name, assignee email, assignee phone number, assignee agency, account user name, account user email, account user phone number The data in the ASPR Ready system will be retained for five years.
PTA -9A:	Are user credentials used to access the system?	Yes
PTA - 9B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS Email Address HHS Password

		HHS/OpDiv PIV Card Non-HHS User Credentials Email address Password
PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	User credential information is collected for authentication. Information related to requestor and assignee is collected for contact/response purposes.
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 10B:	Please specify which PII data elements are used.	Name, email, phone number
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes

PIA

PIA - 1:	Indicate the type of PII that the system will collect or maintain	Name E-Mail Address Phone numbers User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Public Citizens
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	For what primary purpose is the PII used?	Government employees are aware of information collection because it is collected directly from federal employees following the application, hiring, and on-boarding process. Name, email, and phone number is collected for the purpose of submitting and responding to a request. Personally Identifiable Information (PII) will be used only within Assistant Secretary of Preparedness and Response (ASPR). The information (PII) maintained in the system is not shared outside of the federal government.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	Not applicable.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	45 CFR 164.512
PIA - 8:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	OPM/GOVT-1 General Personnel Records
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains In-person Email

		Online Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Other Federal Entities Non-Government Sources Members of the Public Private Sector
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	Government employees are aware of information collection because it is collected directly from federal employees following the application, hiring and on-boarding process. When a user submits a request, they complete the form which requests the user to enter information into fields for their name, email, and phone number in order to submit the request.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason	All individuals are given the opportunity to opt-in to the collection hence no need to provide an opt-out.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained	End users are notified by email when major changes will occur to the system.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not	If an individual believes their data has been misused or is otherwise inaccurate, they may contact the ASPR Ready Help Desk, through which individuals can submit any concern about the program including inaccuracy or misuse of information.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not	User accounts/credentials will be reviewed annually to ensure data's integrity, availability, accuracy, and relevancy.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA-17	Users: HHS employees and direct contractors have PII access to their personal PII only for login purposes. Administrators: System administrators have access for system maintenance and to assist in resolving technical system issues Developers: Development and testing of the system Contractors: Development and testing of the system
PIA - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may	ASPR management approver designees approve ordinary access (i.e., access permitting the

	access PII	routine uses of the data) based on role. ASPR management approver designees have the ability to grant requests for higher level administrative access, but the ASPR management approver designees will approve this level of access based on the requestor's role within the organization, i.e., if the requester has a legitimate business need to access responder records.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job	The system uses role-based security. Roles of users are specifically defined, and the system will grant appropriate levels of access as required by the role or job to be performed.
PIA - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained	All users receive initial user training. There are also HHS mandatory annual courses for all staff on "information systems security awareness" (ISSA), "Privacy Information Awareness" (PIA), and "Records Management" courses as well as contractor security training (corporate-based).
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	The ASPR Ready team will provide specific user training.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	ASPR Ready follows the customer specified retention schedule of five years.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	Administrative: ASPR Ready utilizes role-based security and the ASPR Ready administrators adhere to a least privilege methodology to ensure that all access rights are approved and are specific to the individual's job role. All user accounts are verified and approved 1:1. Technical: All users are required to use multifactor authentication (MFA). Password requirements will be required to adhere to the HHS password policy. ASPR Ready uses HTTPS protocols to encrypt communication with the system. Physical: Servers are maintained in a secure GovCloud environment. Physical access is restricted to only authorized users.
PIA - 25:	Describe the purpose of the web site, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response	The purpose of the web site is to manage communication and requests for ASPR response missions. Users access the system using the public URL (asprready.hhs.gov). Login requires a user to use multifactor authentication to access the internal secure system.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	Yes
PIA - 27A:	Select the type of website measurement and customization technologies is in use and if it is used to collect PII	Session Cookies - Does Not Collect PII
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No