

## Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

## Instructions


Review the following steps to complete this questionnaire:

- 1) Answer questions.** Select the appropriate answer to each question. Question specific help text may be available via the  icon. If your answer dictates an explanation, a required text box will become available for you to add further information.
- 2) Add Comments.** You may add question specific comments or attach supporting evidence for your answers by clicking on the  icon next to each question. Once you have saved the comment, the icon will change to the  icon to show that a comment has been added.
- 3) Change the Status.** You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.
- 4) Save/Exit the Questionnaire.** You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

### 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

<b>PIA Name:</b>	CDC - PMAS - QTR4 - 2023 - CDC7216813	<b>PIA ID:</b>	1745444
<b>Name of Component:</b>	CDC - Performance Management Appraisal System	<b>Name of ATO Boundary:</b>	Performance Management Appraisal System
<b>Overall Status:</b>		<b>PIA Queue:</b>	
<b>Submitter:</b>		<b># Days Open:</b>	58
<b>Submission Status:</b>	Re-Submitted	<b>Submit Date:</b>	12/19/2023
<b>Next Assessment Date:</b>	N/A	<b>Expiration Date:</b>	1/1/2100
<b>Office:</b>		<b>OPDIV:</b>	CDC
<b>Security Categorization:</b>	Moderate	<b>OpDiv PIA ID:</b>	CDC7216813
<b>Legacy PIA ID:</b>		<b>Make PIA available to Public?:</b>	Yes
<b>1:</b>	Identify the Enterprise Performance Lifecycle Phase of the system.		Operations and Maintenance
<b>2:</b>	Is this a FISMA-Reportable system?		Yes
<b>3:</b>	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		Yes
<b>4:</b>	ATO Date or Planned ATO Date.		12/21/2023
<b>5:</b>	Is the system or electronic information collection, agency or contractor operated?		Agency

## PTA

<b>PTA</b>		
<b>PTA - 2:</b>	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
<b>PTA - 2A:</b>	Describe in further detail any changes to the system that have occurred since the last PIA.	N/A
<b>PTA - 3:</b>	Is the data contained in the system owned by the agency or contractor?	Agency
<b>PTA - 4:</b>	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.	<p>Performance Management Appraisal System (PMAS) is an application that focuses on results-oriented performance objectives for each employee that relate to the agency's goals. PMAS is a direct result of the "One HHS" initiative. Under the 20 department-wide objectives, PMAS covers all civil service non-Senior Executive Service (SES) managers, supervisors, and employees, including Title 42 service fellows. Commissioned Corps personnel are not included in this program.</p> <p>PMAS was developed to track employees' performance plans, reviews and ratings and awards. The system also determines award eligibility and allocation information.</p>

**PTA - 5:**

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.

PMAS contains pre-defined elements and standards that track employees' performance plans and reviews, ratings and award allocation information, all organized by job series and grade. The system has extensive calculations in order to determine monetary award amounts given to employees based on their performance ratings. The collection of standards consists of high-level critical elements and performance standards (sub-elements), of which the employees' performance will be rated against at mid-year (where applicable) and end of year.

Employee performance plans, reviews and ratings, and awards are tracked in the system. PMAS does not itself collect or maintain personal information or PII, but instead relies on the employee's data that is collected by the Data Management and Analytics System (DMAS) and the CDC Enterprise Reporting System (ERS) as part of the on-boarding process; this includes name, employment status, salary, pay plan, and grade/series.

The PII is used to track employee performance plans, reviews and ratings, and awards using the employee's name, employment status, salary, pay plan, and grade series.

PMAS users are identified and authenticated using PIV card credentials via Active Directory (AD). AD is a separate system with its own PIA along with DMAS and ERS.

**PTA - 5A:**

Are user credentials used to access the system?

**PTA - 5B:**

Please identify the type of user credentials used to access the system.

<b>PTA - 6:</b>	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.	<p>PMAS focuses on result-oriented performance objectives for each employee that relate to the agency's goals by tracking employee performance plans, reviews and ratings, and awards. PMAS covers all civil service, non-SES managers, supervisors, and employees, including Title 42 service fellows. Commissioned Corps and contractor personnel are not included in this program.</p> <p>PMAS contains pre-defined elements and standards that tracks employees' performance plans and reviews, ratings and award allocation information, all organized by job series and grade to aide supervisors and employees in standardizing language to be used in creating draft Performance Plans. The system has extensive calculations in order to determine monetary award amounts given to employees based on their performance ratings.</p> <p>The system tracks employees' performance plans and reviews, rating and award allocation information. The system has extensive calculations in order to determine monetary award amounts given to employees based on their ratings.</p> <p>Employee performance plans, reviews and ratings, and awards are tracked in the system. PMAS does not itself collect or maintain personal information or PII, but instead relies on the employee's data that is collected by the Data Management and Analytics System (DMAS) and the CDC Enterprise Reporting System (ERS) as part of the on-boarding process; this includes name, employment status, salary, pay plan, and grade/series.</p>
<b>PTA - 7:</b>	Does the system collect, maintain, use or share PII?	Yes
<b>PTA - 7A:</b>	Does this include Sensitive PII as defined by HHS?	Yes
<b>PTA - 8:</b>	Does the system include a website or online application?	Yes
<b>PTA - 8A:</b>	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
<b>PTA - 9:</b>	Describe the purpose of the website, 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.	CDC staff access the website at pmas.cdc.gov. One primary purpose of the website is to determine award eligibility and allocation information for CDC staff. PMAS users which includes direct contractors are identified and authenticated using PIV card credentials via Active Directory (AD). AD is a separate system with its own PIA along with DMAS and ERS.
<b>PTA - 10:</b>	Does the website have a posted privacy notice?	Yes
<b>PTA - 11:</b>	Does the website contain links to non-federal government websites external to HHS?	No
<b>PTA - 11A:</b>	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
<b>PTA - 12:</b>	Does the website use web measurement and customization technology?	No

<b>PTA - 12A:</b>	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
<b>PTA - 13:</b>	Does the website have any information or pages directed at children under the age of thirteen?	No
<b>PTA - 13A:</b>	Does the website collect PII from children under the age thirteen?	
<b>PTA - 13B:</b>	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
<b>PTA - 14:</b>	Does the system have a mobile application?	No
<b>PTA - 14A:</b>	Is the mobile application HHS developed and managed or a third-party application?	
<b>PTA - 15:</b>	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
<b>PTA - 16:</b>	Does the mobile application/ have a privacy notice?	
<b>PTA - 17:</b>	Does the mobile application contain links to non-federal government websites external to HHS?	
<b>PTA - 17A:</b>	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
<b>PTA - 18:</b>	Does the mobile application use measurement and customization technology?	
<b>PTA - 18A:</b>	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
<b>PTA - 19:</b>	Does the mobile application have any information or pages directed at children under the age of thirteen?	
<b>PTA - 19A:</b>	Does the mobile application collect PII from children under the age thirteen?	
<b>PTA - 19B:</b>	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
<b>PTA - 20:</b>	Is there a third-party website or application (TPWA) associated with the system?	No
<b>PTA - 21:</b>	Does this system use artificial intelligence (AI) tools or technologies?	No

## PIA

### PIA

<b>PIA - 1:</b>	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Employment Status Other - Free text Field - Employee Rating, Salary, Pay Plan and Grade Series
<b>PIA - 2:</b>	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
<b>PIA - 3:</b>	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
<b>PIA - 4:</b>	For what primary purpose is the PII used?	The PII is used to track employee performance plans, reviews and ratings, and awards using the employee's name, employment status, salary, pay plan, and grade series.
<b>PIA - 5:</b>	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None

<b>PIA - 6:</b>	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	None
<b>PIA - 6A:</b>	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	None
<b>PIA - 7:</b>	Identify legal authorities governing information use and disclosure specific to the system and program.	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347
<b>PIA - 8:</b>	Are records in the system retrieved by one or more PII data elements?	Yes
<b>PIA - 8A:</b>	Please specify which PII data elements are used to retrieve records.	Name, Salary and Pay Plan
<b>PIA - 8B:</b>	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-2 Employee Performance File System Records
<b>PIA - 9:</b>	Identify the sources of PII in the system.	Government Sources Within the OPDIV
<b>PIA - 10:</b>	Is there an Office of Management and Budget (OMB) information collection approval number?	No
<b>PIA - 10A:</b>	Provide the information collection approval number.	
<b>PIA - 10B:</b>	Identify the OMB information collection approval number expiration date.	
<b>PIA - 10C:</b>	Explain why an OMB information collection approval number is not required.	N/A. No information is collected from the public
<b>PIA - 11:</b>	Is the PII shared with other organizations outside the system's Operating Division?	No
<b>PIA - 11A:</b>	Identify with whom the PII is shared or disclosed.	
<b>PIA - 11B:</b>	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
<b>PIA - 11C:</b>	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
<b>PIA - 11D:</b>	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
<b>PIA - 12:</b>	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
<b>PIA - 12A:</b>	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	Collection of individuals is
<b>PIA - 13:</b>	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	The PII is collected as part of the individual's in-processing as a condition of employment with the CDC, and as such, there is no option to object to its collection.
<b>PIA - 14:</b>	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.	Major changes to the information system are published to the user community and individuals via employee announcements and information published to the CDC intranet.

<b>PIA - 15:</b>	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.	Individuals having concerns regarding the use or accuracy of their information should contact the Technology Services Branch (TSB) Help Desk or by submitting a Service Now (SNOW) ticket online: <a href="https://servicedesk.cdc.gov/">https://servicedesk.cdc.gov/</a> .  They may also contact the CDC Computer Security Incident Response Team (CSIRT) at the 24 x 7 Emergency Number (1-866-655-2245) and then with a follow-up email to csirt@cdc.gov.
<b>PIA - 16:</b>	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.	The PII is collected as part of the individual's in-processing with the CDC, stored in a common database and accessed by PMAS. Any changes to the common database are immediately reflected in PMAS ensuring the system data's integrity.
<b>PIA - 17:</b>	Identify who will have access to the PII in the system.	Users  Administrators  Developers  Contractors
<b>PIA - 17A:</b>	Select the type of contractor.	HHS/OpDiv Direct Contractors
<b>PIA - 17B:</b>	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	No
<b>PIA - 18:</b>	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	The PII is collected as part of the individual's in-processing with the CDC, stored in a common database and accessed by PMAS. Any changes to the common database are immediately reflected in PMAS ensuring the system data's integrity.  Users: Users have access to review individual information  Administrators: Access to input employee ratings into the system  Developers: Access for System maintenance and upgrades  Contractors: Direct contractors require access to input employee ratings into the system
<b>PIA - 19:</b>	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	PMAS uses the Role-Based Access Control (RBAC) to restrict a user's ability to view PII to only that required to perform their job function. The roles are assigned by supervisors and implemented by the TSB Help Desk in the RBAC application authorization server.
<b>PIA - 20:</b>	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.	PMAS uses RBAC to restrict a user's ability to view PII to only that required to perform their job function. The roles are assigned by supervisors and implemented by the TSB help desk in the RBAC application authorization server.

<p><b>PIA - 21:</b></p>	<p>Identify the general security and privacy awareness training provided to system users (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.</p>	<p>Users must undergo annual Security and Privacy Awareness Training to maintain their CDC network account and access to PMAS.</p>
<p><b>PIA - 22:</b></p>	<p>Describe the training system users receive (above and beyond general security and privacy awareness training).</p>	<p>None</p>
<p><b>PIA - 23:</b></p>	<p>Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).</p>	<p>All official records are transferred or destroyed based on CDC record management policies and practices. The following records schedules apply to the system:</p> <p>GRS 2.2.070 Destroy no sooner than 4 years after date of appraisal, but longer retention is authorized if required for business use</p> <p>GRS 2.2.071 . Destroy after employee completes 1 year of acceptable performance from the date of written advance notice of proposed removal or reduction-in-grade notice. This disposition instruction is mandatory; deviations are not allowed.</p>
<p><b>PIA - 24:</b></p>	<p>Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.</p>	<p>Administrative: Records are maintained according with CDC's record control schedule and record control policy. The PII is secured using CDC Active Directory authentication process and Role-Based Application Controls.</p> <p>Technical: Monitored by the Network and IT security controls which is administered by Cybersecurity Program Office (CSPO) and Digital Solutions Office (DSO). Information is exchanged with HHS across an encrypted file transfer connection.</p> <p>Physical: Locations are protected by security guards, with access controlled by ID badges and key card restrictions.</p>

## Review & Comments

### Privacy Analyst Review

<b>OpDiv Privacy Analyst Review Status:</b>	Approved	<b>Privacy Analyst Review Date:</b>	12/21/2023
<b>Privacy Analyst Comments:</b>	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: December 21, 2023	<b>Privacy Analyst Days Open:</b>	

### SOP Review

<b>SOP Review Status:</b>	Approved	<b>SOP Signature:</b>	
<b>SOP Comments:</b>	Approved on behalf of Beverly Walker	<b>SOP Review Date:</b>	1/23/2024
		<b>SOP Days Open:</b>	35

### Agency Privacy Analyst Review

<b>Agency Privacy Analyst Review Status:</b>	Approved	<b>Agency Privacy Analyst Review Date:</b>	1/26/2024
<b>Agency Privacy Analyst Review Comments:</b>	Reviewer: Nestor Villafuerte This PIA is ready for SAOP review and approval.	<b>Agency Privacy Analyst Days Open:</b>	3

### SAOP Review

<b>SAOP Review Status:</b>	Approved	<b>SAOP Signature:</b>	Archer Signature_Bridget Guenther.docx
<b>SAOP Comments:</b>	PTA 5 is blank, please update with next iteration of the PIA.	<b>SAOP Review Date:</b>	2/7/2024
		<b>SAOP Days Open:</b>	12

### Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA - 8B	Data Feed Service, piafrmdc	12/14/2023	<p>Need to cite a System of Records Notice (SORN)</p> <p>Previously approved PIA cited "OPM/GOVT-2, Employee Performance File System Records". Please speak with your Center's Records Officer to learn more.</p>	
PIA - 10C	Data Feed Service, piafrmdc	12/14/2023	OMB Collection Approval numbers refer to collection of information sourced from the public.	
PIA - 18	Data Feed Service, piafrmdc	12/14/2023	<p>Please describe why each category of user requires access. Can organize as follows:</p> <p>User: Reason for access. May include contractors.</p> <p>Developer: Reason for access. May include contractors.</p> <p>Administrator: Reason for access. May include contractors.</p> <p>Contractor: Reason for access. Note if they serve as user, developer, and/or administrator.</p>	
PIA - 24	Data Feed Service, piafrmdc	12/14/2023	OCISO and ITSO are outdated acronyms. Please update and list examples of actual technical controls in use.	
PIA - 23	VILLAFUERTE, NESTOR	1/24/2024	Please define the acronym "GRS" in its first instance.	
PIA - 1	BLAND, CRYSTAL	1/26/2024	<p>Update on the next iteration of the PTA:</p> <p>PTA-5A: Please select "Yes, but user credentials are maintain by another system...."</p>	
PIA - 1	Data Feed Service, piafrmdc	9/30/2024	This System has been migrated within the OCIO ISB Infrastructure Services authorization boundary. All future updates should be made via the new Sub- Component application.	

### Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	Is OpDiv Privacy Analyst Return ? :	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	Is Agency Privacy Analyst Return ?:	0
Is SAOP Approved?:	1	Is SAOP Return ?:	0
Total Approved:	4	Total Return:	0
Total Approval Required:	4		

### Miscellaneous Fields

Last Updated:	9/30/2024 8:01 PM	History Log:	<a href="#">View History Log</a>
---------------	-------------------	--------------	----------------------------------