PTA / PIA: OS - PACS PSEMS - QTR1 - 2026 - OS3293257

Created Date: 2/13/2026 8:04 PM Last Updated: 2/26/2026 8:23 PM

General Information

PTA / PIA Name:	OS - PACS PSEMS - QTR1 - 2026 - OS3293257	**PTA / PIA ID:**	4267610
Component Name:	OS - OS - OS - Physical Access Control System Physical Security Emergency Management Safety	**ATO Boundary Name:**	Physical Access Control System Physical Security Emergency Management Safety
Overall Status:	Complete	**# of Days - Open:**	22
Submitter:		**Submit Date:**	2/11/2026
Next Assessment Date:	02/25/2029	**Expiration Date:**	2/25/2029
Office:		**OpDiv:**	OS
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	11/30/2026
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Janet Bass
PTA 01A:	POC Title and Organization	ESS/LOB ISSO
PTA 01B:	POC Email Address	janet.bass@hhs.gov
PTA 01C:	POC Phone Number	301-852-9329
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The PIA was about to expire, this is an update
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	Physical Access Control System Physical Security Emergency Management Safety (PACS PSEMS) is an access control application designed to grant, monitor, and maintain physical access of individuals to the All HHS Office of the Secretary (OS) buildings in the HHS Complex.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The information in the system is maintained for the purpose of granting physical access of individuals to all HHS OS buildings in the southwest complex. PACS PSEM collects and maintains personally identifiable information (PII) (name, photo, employee office location, employee number (Personal Identifier), and Federal Agency Smart Credential Number (FASC-N)) for the purpose of printing Personal Identity Verification (PIV) cards and generating access requests. In order to be granted the appropriate request, each individual (Federal & contractor employee) is required to submit this personal information at the time employment is accepted as part of the on-boarding process via a badge request form (form number, 828). The FASC-N is generated when the card is printed. PIV cards are not printed for non-federal visitors. Nonfederal visitors are required to provide a photo ID which is used to print a temporary paper badge containing name and photo. This Personal Identifiable Information (PII) is stored for two years. PIV card credentials are the user credentials for System Administrators. These credentials are used to access the PACS PSEM system, but are not collected or maintained in the system, PACS PSEM. The system collects and stores the following information for system administrator: username, password, HHS ID and email. No 'biometric identifiers', 'vehicle identifiers', Date of Birth, or addresses are collected, maintained, or shared in the PACS PSEM system. The PII that is maintained in the PACS PSEM system originates in the HHS Identity and Access Management (IAM) system which is managed by a contractor. SCMS and IAM maintain their own PIAs. It is extracted from SCMS by the Smart Card Management System (SAFE) database and passed to the PACS PSEM system where it is stored on a Lenel OnGuard database. SAFE is owned and operated by a third-party vendor, Deloitte. No reports containing PII are generated from the PACS PSEM system.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card

PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The PACS PSEM system is an access control application designed to grant, monitor, and maintain physical access to the buildings in the southwest complex. PACS PSEM collects and maintains personally identifiable information (name, photo, employee office location, employee number (Personal Identifier), and Federal Agency Smart Credential Number (FASC-N)) for the purpose of printing Personal Identity Verification (PIV) cards and generating access requests. This occurs by comparing the PII encoded into PIV cards with information contained within HHS's IAMS, to which PACS PSEM is connected. Users swipe their PIV card, and that information is validated by PACS PSEM. If necessary, individuals can be directed to a booth where a temporary paper badge, containing name and photo only, can be created; also using PACS PSEM. PII is submitted by the employees themselves as part of the onboarding process. Non-federal visitors are required to provide a photo ID which is used to print a temporary paper badge containing name and photo only. PACS PSEM also records 'events' (irregularities) and provides alerts (notifications where access authorization appears incorrect or inappropriate).
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Employee ID Number Biographical Information Name Biometrics/Distinguishing Features Photographic Identifiers Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Free text Field - Others - Operating Division, Staff Division Federal Agency Smart Credential Number (FASC-N) and employee office location
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)

PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100,000 – 999,999
PIA 25:	For what primary purpose is the PII used?	Information is used to confirm identity and to verify the , Personal Identity Verification (PIV) card/badge holder has permission to enter certain Health and Human Services (HHS) facilities.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	Personally Identifiable Information (PII) is not used for secondary purposes.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Primarily Homeland Security Presidential Directive 12 (HSPD-12) calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors. System of Records Notice (SORN) 09-90-0777
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	The PII elements are retrieved by PIV card whenever possible, if the user does not have a PIV card building access data can be retrieved by First and Last Name.
PIA 29B:	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.	Primarily Homeland Security Presidential Directive 12 (HSPD-12) calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors. System of Records Notice (SORN) 09-90-0777
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax Government Sources Other HHS OPDIV Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	The system does not collect PII as it comes from Identity and Access Management System (IAMS), Identity and Access Management System (IAMS), is the PII owners.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Information is collected directly from individuals. Consent is granted as part of the employee (Federal & Contractor) on-boarding process via Form 828. The PII that is maintained in the PACS PSEM system originates in the HHS Smart Card Management System (SCMS) (called Identity and Access Management (IAM) system) and it is the responsibility of the source system for when/ if individuals opt-out of the collection of use of their PII. Although the use of PII is implicit in the employer/employee relationship, and for all those entering the facilities, a System Of Records Notice (SORN) is required under the Privacy Act, and will be used to describe any use of an Individual's PII for purposes materially different from that given at the time of collection. There is no option to opt out because it is part of the employee/employer relationship and it established during the on-boarding process.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	Individuals would be notified via email of major system changes that affect their rights or interests. Major changes would also be reflected by updates to the SORN
PIA 36:	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 who believe their PII is inaccurate or incomplete can contact the HHS badging office or otherwise identify the appropriate system owner to correct or amend the information.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	There is not a process in place to conduct periodic reviews as the information (PII) resides in Identity and Access Management System (IAMS), which is updated periodically. The review of PII falls under the responsibility of IAMS, as the information is pulled from individuals' PIV cards. PACS PSEM downloads information from IAMS to a LENEL OnGuard database. LENEL is the brand name of the access control database used by PACS PSEM. The source system is updated on a regular basis and the data is downloaded.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: Access to Personally Identifiable Information (PII) available based on rights assigned by the Administrators. Necessary for assigning access rights to HHS occupied buildings. Users have different levels of access based on their role and duties. Administrators: Responsible for assigning access rights to other users. Developers: Full access to system. Responsible for application updates. Contractors: Direct Contractors have full access to system. Responsible for application updates, data base administration, and system administration.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrators, developers, and contractors have access to PII. Access levels are provided and restricted based on the user's role and/or time constraint. Access is repealed via receipt of an e-mail request from authorized management staff.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Role based permission based on job function and responsibility. Administrators have access to all records.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	The Office of Security and Strategic Information (OSSI) complies with the Federal Information Security Management Act (FISMA) requirement to be exposed to security awareness materials, at least annually and prior to employee's use of, or access to, information systems by communicating directly with individuals who access the system. This training includes the annual HHS Privacy and Security Awareness training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	In addition to the general security and privacy awareness training, system users receive on the job training.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	General Records Schedule (GRS) 5.6. Item 120, Disposition Authority: DAA-GRS-2021-0001-0005. Temporary. Destroy 6 years after the end of an employee or contractor’s tenure, but longer retention is authorized if required for business use. When there are employment status changes, data is removed from the LENEL database.

PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	PII is secured using: Administrative controls include roles and responsibilities to provide for access using the concepts of least privileges and separation of duties. Access levels are provided and restricted based on the user's role and responsibilities. Accreditation activities are performed to ensure security controls are in place and operating as designed. Technical controls are in place to limit access to only those requiring it and only for those purposes intended and authorized by the System Owner. These include UserID, password, IDS (Intrusion Detection System) and firewalls. Physical controls to the system are provided by the Office of Information Technology Infrastructure and Operations (ITIO) and include security guards, Identification badges, key cards, cipher locks and Closed-Circuit TV (CCTV).

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	2/11/2026
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	2/13/2026
SOP Review Comments:		**# of Days - SOP Review:**	2

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	2/17/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 2/17/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	4

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	2/26/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	9

SAOP Signature

Date	User	Type	Name	Original Value	New Value
2/26/2026 2:36 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 04	Data Feed Service, pta_pia_OS_Release	2/11/2026	Please define PACS PSEM on first use within this response.	
PTA 05	Data Feed Service, pta_pia_OS_Release	2/11/2026	Please define LENEL on first use within this response.	
PIA 22A	Data Feed Service, pta_pia_OS_Release	2/11/2026	Please also include 'employee office location'.	
PIA 37	Data Feed Service, pta_pia_OS_Release	2/11/2026	This response appears to be a copy of the previous response to a different question. Please update this response. For reference, here is the information provided in the previous approved version of the PIA: There is not a process in place to conduct periodic reviews as the information (PII) resides in Identity and Access Management System (IAMS), which is updated periodically. The review of PII falls under the responsibility of IAMS, as the information is pulled from individuals' PIV cards. PACS PSEM downloads information from IAMS to a LENEL OnGuard database. LENEL is the brand name of the access control database used by PACS PSEM. The source system is updated on a regular basis and the data is downloaded.	
PTA 05	Data Feed Service, pta_pia_OS_Release	2/11/2026	Additional note: Lenel is a company name it is not an acronym.	