US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/22/2016

OPDIV:

CMS

Name:

Electronic Security System

PIA Unique Identifier:

P-7451413-074662

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Electronic Security System (ESS) supports CMS physical security through information systems that govern video monitoring, electronic access to secure areas, visitor management, occupant emergency organization, incident reporting, risk assessment, headquarters building parking, and compliance with the requirements of Homeland Security Presidential Directive 12 (HSPD-12).

Describe the type of information the system will collect, maintain (store), or share.

Data collected includes full name, address, phone number, e-mail address, Personal Identity Verification (PIV) card data such as Federal Agency Smart Card-Number (FASC-N) and certificate data, Facial Photograph, video and vehicle information. Additionally, employees with disabilities information is being voluntarily collected from Federal Employees and direct Contractors for those requiring assistance out of CMS facilities in the event of an emergency evacuation. Additionally, foreign national status; organization; position; disability status; FASC-N; PIV card number may be collected and maintained.

Information collected from users/system administrators in order to access the system consists of user credentials (username, password, and Personal Identity Verification PIV card data). Users/system administrators include CMS employees and direct contractors.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The Electronic Security System (ESS) is a General Support System (GSS) with Major Applications. It is comprised of four main subsystems: the General Support System (GSS), Physical Access Control (PACS), Closed-Circuit Television System (CCTV) and the Physical Access Management (PAM). The ESS is not a publicly available system. All users are either CMS employees or direct contractors. Additionally, foreign national status; organization; position; disability status; FASC-N; PIV card number may be collected and maintained.

These subsystems combine to support the Personal Identity Verification (PIV) process, control physical access to CMS facilities, visitor management, parking, physical security facility risk assessment, the occupant emergency organization, alarm monitoring, physical intrusion detection, video monitoring and post-incident response.

Below describes that data used in each subsystem:
GSS - PII collected from users/system administrators in order to access the system, consists of user credentials (e.g. username, password, and Personal Identity Verification (PIV) card data). Users/system administrators include CMS employees and direct contractors.

PACS - full name, PIV Card FASC-N and certificate data as well as facial image. This information is used for physical access to CMS facilities and limited access spaces within CMS facilities.

CCTV - This subsystem collects and stores video surveillance of CMS facilities and entrances to limited access spaces within CMS facilities.

PAM - PAM consists of multiple modules, each of which collects and uses data for the following specific purposes:

Parking - full name, Group, Position Title, email address, Building, Desk Location, Phone, Lot, Work schedule, and Vehicle information. All fields are optional unless the individual is requesting a medical, carpool or executive parking permit, in which case, all fields are required. Medical parking requests additionally collect affilation, State Disability soundex number and image of MVA disability parking certification card and expiration date all of which are required. Carpools additionally require the collection of the home address for each carpool member.

Occupant Emergency Organization (OEO) - full name, phone number, email address, region, OEO Position, Assembly Area, Zone, Building, Location, and Office. All are optional fields. Individuals may also self identify as an Employee with Disabilities (EWD) to receive an EWD monitor for assistance in emergencies. This is optional.

PACS Central - full name, facial image, email address, access level information, PIV Card FASC-N and PIV Card certificate data. This information is used for electronically requesting, approving and reviewing access to CMS facilities and limited access spaces.

Welcome Center - visitor full name, visitor foreign national status, visitor organization, type of identification presented for access, date of visit, purpose of visit, building, escort, visitor badge number issued and date and time visit ended. This information is used to track visitors at CMS facilities.

Security Assessment - This is a private module used by the Division of Physical Security and Strategic Information (DPSSI) for evaluating risk compliance at CMS facilities. Information collected is facility-related only and does not contain any information about individuals. Information includes facility security level, threat levels, comments and uploads of supporting documentation.

CMS Incident Management (CIMS) - Originator, originator phone, originator email address, duty station, method of reporting, event date and time, event type, and event location(s). Optional data includes property involved, first and last name of involved CMS employees or direct contractors, vehicle information and event summary/comments.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

Photographic Identifiers

Vehicle Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Certificates

Other: Image of MVA Disability Certification for Medical Parking and HHS User Credentials; foreign

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The PII is used in the following ways: for identity verification purposes for physical access control to CMS facilities, for the issuance of medical and carpool parking permits, for contacting vehicle owners in the event of an emergency, to support the assistance of self-identified employees with disabilities with evacuation from CMS facilities, for the authentication of system and subsystem users.

Describe the secondary uses for which the PII will be used.

There are no secondary uses for the PII

Identify legal authorities governing information use and disclosure specific to the system and program.

Homeland Security Presidential Directive-12 (HSPD-12); 5 USC 301, Departmental Regulations

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-70-0529 Employee Building Pass Files

09-70-0515 Record of Individuals allowed Regular and Special Parking Privileges at the CMS

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Other Federal Agencies

The ESS sends the minimum data required to access a physical access control system (PACS) to federal offices where CMS does not control the PACS system which grants access to CMS employees and direct contractors. This is a one-time file of data containing the employee's name and PIV Card data whenever a PACS system is installed or replaced by the agency controlling physical access to a CMS space (e.g. The Social Security Administration controls physical access to the CMS Dallas Regional Office. A listing of CMS Dallas employees was sent to populate the PACS system).

Describe any agreements in place that authorizes the information sharing or disclosure.

There is an Information Sharing Agreement (ISA) with HHS regarding the SCMS to ESS web services connection.

Describe the procedures for accounting for disclosures.

For individual requests of data, the ESS maintains the following information on the ESS Documentation SharePoint Repository in the Data Disclosure Log:

Date, nature, and purpose of each disclosed record; and the Name and address of the person or agency to which the disclosure was made.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Individuals are notified at the time of collection. Each module/data form contains language similar to the following:

Your response to the questions on this form is not required by law. However, if you do not provide this information, your application for privileges may be denied or delayed in processing. No disclosure of this information will be made without your written consent unless required by law or required for routine badge issuance use.

The information on this form is collected, maintained and used for assigning, controlling, tracking and reporting any permanently or temporarily issued unescorted or restricted access into CMS facilities and for issuing and contorlling any type of access card for electronically-controlled physicall space in CMS facilities.

ESS also collects user ID and password from CMS employees and direct contractors in order to log into the system. However these login credentials (User Id and Password) are provided to HHS credentialed users who have been notified of the collection of their PII during the onboarding and new employee intake process.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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.

While a response to the questions on ESS Forms is not required by law, individuals who do not provide this information for certain modules could see their privileges for physical access denied or delayed in processing. Individuals are informed of this on ESS Forms. There is no formal method to opt-out on the minimum set of data required to process ESS forms.

System users cannot 'opt-out' of providing login credentials (user ID and Password). The login credentials are needed to grant access to ESS.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The ESS has the ability to send email notification to individual's whose data is stored in an ESS system should a disclosure occur or data use change.

System users will be notified via email if any major changes were to occur to the use and disclosure of their PII. There is no process to consent as the information is necessary in order to perform their job.

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.

The ESS System offers Microsoft Outlook resource mailboxes for each subsystem and subsystem module for redress issues. Any data that is related to the PIV card enrollment/issuance process is directed to the Division of Personnel Security Services (DPSS) for redress.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Individual users are requested to review some of their ESS information on an annual basis. For physical access, records are reviewed on a quarterly basis by a designated official known as a Room Owner or their assigned Access Authorities. The ESS also receives real time event notification whenever a user's PIV record changes (e.g. name change, re-issued, renewed, revoked) and takes action according to the type of event. For authentication data, system logs are reviewed daily for suspicious activity and users are required to change passwords every 60 days. ESS back-up servers are in place to ensure information is readily available, even if a main server fails.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Some users are required to review lists of people who have access to their assigned areas within the building.

Administrators:

Administrators require the need to search all records.

Contractors:

Guard staff are direct contractors and are required to validate identity of people entering CMS facilities. Additionally, some contractors are Administrators who are direct contractors with CMS credentials.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Access to PII is based on the role that each system user must perform within the system. Each module supports these roles and each role is customized based on its module to limit which PII data element(s) are accessible to that role. Users must complete a request form for access to all ESS system roles which is then reviewed and approved by the appropriate system administrator.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Users are assigned roles within the system and each role is associated with the minimum set of privileges required to carry out the tasks for that role. The system also audits and requires digital signatures for specific operations within the system.

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.

Each employee and contractor with access to CMS systems is required to take general CMS security and privacy awareness training annually.

Describe training system users receive (above and beyond general security and privacy awareness training).

Training on user roles is performed whenever a new user is granted access to the ESS. Training is also provided to users whenever a system change warrants the need for training. This need is assessed during the change management process and performed prior to the system change taking affect. Additionally, Contingency Plan exercises and Incident Response training are performed annually.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Data is retained in accordance with NARA and CMS guidelines as follows:

Delete/destroy when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes (N1-GRS-95-2 item 1c).

Profile data. Delete an individual's profile 1 year after individual separates from agency (N1-64-08-6, item 1).

Badging and access control activity data. Cut off semiannually. Delete 6 months after cutoff (N1-64-08-6, item 2).

System documentation. Destroy when revised OR superseded (N1-64-08-6, item 3).

Disaster recovery backup files. Delete when 60 days old (N1-64-08-6, item 4)."

Privately owned facilities. Reports and related records, including surveys and inspections of privately owned facilities assigned security cognizance by Government agencies. Cut off annually. Destroy when 4 years old OR when security cognizance is terminated, whichever is SOONER. (GRS 18, item 10).

GRS 20, item 13 and 14 - "Word Processing Files. Delete from the word processing system when no longer needed for updating OR revision (GRS 20, item 13).

E-mail Records. Delete from the e-mail system after copying to a recordkeeping system (GRS 20, item 14).

User Identification, Profiles, Authorizations, and Password Files, EXCLUDING records relating to electronic signatures. Destroy/delete inactive file 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later (N1-GRS-03-1 item 6a).

Electronic files and hard copy printouts created to monitor system usage. Delete/destroy when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes (N1-GRS-95-2 item 1c).

The Electronic Security Systems retains audit trail files for a minimum of one year.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

The ESS system is housed in a limited access area of CMS. Only a limited number of people are authorized to enter this space and the list of authorized people is reviewed quarterly. Any visitors escorted into the space are required to sign the visitor's log which is also reviewed quarterly.

The ESS PAM subsystem stores PII data on self-encrypted disks. So data at rest is encrypted. Additionally, data in transmit between the application server, PACS subsystem and database server are encrypted via SSL. There is a physical firewall between the ESS PAM application and database servers.