US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/31/2024

OPDIV:

NIH

Name:

CUP Personnel Management Systems (CPMS)

PIA Unique Identifier:

P-3814944-152082

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

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 Office of Research Facilities (ORF) Central Utility Plant (CUP) Personnel Management Systems (CPMS) is a National Institutes of Health (NIH) information system used for personnel safety and sending emergency notification in a situation when security concern happen such as fire, gun attack, and system failure. The CPMS system is comprised of the following four components:

Mass Notification System (MNS): The function of MNS is to send mass notification in case of fire, gun attack, and system failure. The notifications are audible emergency alerts to CUP personnel. Alerts are manually triggered from one of four dedicated control panels located in high traffic areas of the CUP. The system resides on an islanded network of speakers forming a public address system. SmartView software is used to configure and maintain the ADVANCE system and its network; consisting of various hardware intercom system components (master control unit, input modules, handsets, amplifiers, speakers, and beacons).

Real Time Locating Services (RTLS): RTLS is a camera system that collects people’s movement in

the CUP and the status of assets and tools in it and reports back to security personnel. RTLS application is used for real-time tracking of people, asset, tool. RTLS Ultra White Band (UWB) tags placed on equipment and/or personnel to wirelessly emit location data, which is collected by RTLS nodes. RTLS nodes are FACnet connected and transmit data to the RTLS UWB core. Data stored in the RTLS-UWB core is made available to the Input output (IO) platform which manages devices (collect, process, and perform analytics) and visualize data for end user operation.

Visitor Management System (VMS): The VMS is the primary personnel tracking database for the CUP. The purpose of the system is to monitor visitors of the CUP and maintain a record of all personnel entering and exiting from the building to maintain readiness during emergency situations as well as accurate documentation of the visitor's log. The main reception station is the physical hub of the VMS. All visitors needing a badge are required to visit the main reception station to check in as this is the only station with a available paper badge printer. All personnel entering and exiting the building will be required to scan their badge (paper or plastic) on each entry and exit regardless of the number of times that the action is repeated in a single day.

Emergency Notification System (ENS): ENS is a hybrid application. It is part of VMS and the merging point between MNS and RTLS (middle point). The system is used to notify all Division of Technical Resources (DTR) personnel and current visitors within a 24-hour period who have checked in using the VMS system via text/email of the event of an emergency at the CUP. Only privileged users can send a Emergency Communication Message.

RTLS Camera collect people's movement in the CUP and the status of assets and tools. ENS and MNS utilize VMS information such as email and phone for Emergency notification.

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

The type of personally identifiable information (PII) that CPMS collects and maintains are: Visitors' names, photograph, Email, phone numbers, and sensor data.

Administrators log in to RTLS, MNS, and ENS via system specific username and password. Users log in and log out of VMS using their phone number. Users need to register to VMS using name, email, and phone number in order to access it.

All CPMS systems are located in a secured zone where only authorized users have access with their NIH Personal Identity Verification (PIV) Card.

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

The ORF CPMS is a NIH information system used for personnel safety and emergency notification in a situation when security concern happen such as fire, gun attack, and system failure. The CPMS system is comprised of the following four components:

MNS: The function of MNS is to send mass notification in case of fire, gun attack, and system failure. The notifications are audible emergency alerts to CUP personnel. Alerts are manually triggered from one of four dedicated control panels located high traffic areas of the CUP. The system resides on an islanded network of speakers forming a public address system.

RTLS: RTLS is a camera system that collects people's movement in the CUP and the status of assets and tools in it and reports back to security personnel. RTLS application is used for real-time tracking of people, asset, tool . RTLS UWB tags placed on equipment and/or personnel to wirelessly emit location data, which is collected by RTLS nodes. Data stored in the RTLS-UWB core is made available to the IO platform which manages devices (collect, process, and perform analytics) and

visualize data for end user operation.

VMS: The VMS is the primary personnel tracking database for the CUP. The purpose of the system is to monitor visitors of the CUP. The system's intention is to monitor and maintain a record of all personnel entering and exiting from the building to maintain readiness during emergency situations as well as accurate documentation of the visitor's log.

ENS: ENS is a hybrid application. It is part of VMS and the merging point between MNS and RTLS (middle point). The system is used to notify all DTR personnel and current visitors within a 24-hour period who have checked in using the VMS system via text/email of the event of an emergency at the CUP. Only privileged users can send a Emergency Communication Message.

The type of PII that CPMS collects and maintains are: Visitors' names, photograph, Email, phone numbers, and sensor data.

Administrators log in to RTLS, MNS, and ENS via system specific username and password. Users log in and log out of VMS using their phone number to access it. Users need to register to VMS using name, email, and phone number in order to use it.

All CPMS systems are located in a secured zone where only authorized users have access with their NIH PIV Card.

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
E-Mail Address
Phone Numbers
Sensor data
Username and password

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

Employees
Public Citizens
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Emergency notification/response and personnel safety.

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

N/A

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

42 U.S.C. 241, 44 U.S.C. 3101 and 3102, 5 U.S.C. 301 and 302,
5 U.S.C. 7902.

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.

9–25–0166 Administration: Radiation and

09–25–0216 Administration: NIH Electronic

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within the OPDIV

Identify the OMB information collection approval number and expiration date

The Utilities Generation Branch (UGB) is in the process of getting Office of Management and Budget (OMB) clearance. An OMB number and its expiration date will be added when issued.

Is the PII shared with other organizations?

No

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 in person when the information is collected during their first visit to the CUP. Visitors agree to consent on the system use of their PII at the time of registration.

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.

In order to enter the CUP, individuals are required to provide their information for security purposes. Individuals are given the choice to leave the CUP if they are not comfortable giving their information.

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

If any changes made to the system, users will be notified via email or phone number they have provided during registration.

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.

Individuals can contact the system owner when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

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

To ensure the data's integrity, availability, accuracy and relevancy, the system administrator will review the PII contained in the system on weekly and monthly-basis, as needed.

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

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

Administrators , developers, and security personnel access to the system is determined based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job

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.

They access PII only when required to perform their job. Access to PII is assigned to personnel based upon current job responsibilities.

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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

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

Annual information security Awareness and system owners Training. Mandatory security training such as Occupational Safety and Health Administration 30 (OSHA30).

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.

NIH Record retention schedule is used for record maintenance and disposal.

09-412, Facility security management operations records: Records about detecting potential security risks, threats, or prohibited items carried onto federal property or impacting assets.
Disposition Instruction: Destroy when 30 days old, but longer retention is authorized if required for business use.
Disposition Authority: DAA-GRS-2021-0001-0003

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

Physical Controls: The IT hardware used to host protected
information is located in a secured data center facility. The facility is only open to authorized

personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT
systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.