US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/22/2016

OPDIV:

CMS

Name:

CMS Communication System

PIA Unique Identifier:

P-4552937-718554

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 CMS Communication System (CCS) is an internal CMS communication system for use at the CMS Baltimore Regional offices. CCS has three systems for communicating information to CMS employees and contractors. The systems are Digital Signage (DS), Crestron Room View (CV) and the Occupant Emergency Organization and Security Alert System (OEOSAS).

The CCS systems provide news and information to employees, assist with the utilization of conferencing space within CMS and send messages and information to multiple devices (desk phone, mobile phone, email).

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

CCS receives CMS employee and contractor information from the CMS Lightweight Directory Access Protocol (LDAP). The information that is received and stored in CCS is employee name, email address, phone numbers and work locations.

CCS uses information about the CCS administrators and system support staff to allow access to the system. This information includes their name, Enterprise User Administration (EUA) user ID and password.

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

CCS is an internal CMS communications system that is comprised of three components which facilitate communication to CMS employees and contractors. In order to communicate and send messages, CCS stores CMS employee and contractor contact information. Contact information is maintained for the length of employment or deployment in the locations with which CCS communicates.

The Digital Signage (DS) system provides an alternate means of communication to the internal CMS email newsletter called "This Just In." DS information is on video displays throughout buildings to disseminate general employee communications, building event notifications, and live events.

Crestron RoomView (RV) improved the Microsoft Outlook scheduling process. RV reads appointments from Outlook which is displayed on touch panels outside of conference rooms. RV also consists of an Outlook Add-in, which allows a user to schedule a room based on availably and the assets (i.e. Video Teleconference (VTC), projector, whiteboard) located in the room.

Occupant Emergency Organization and Security Alert System (OEOSAS), a Federal Signal product that allows for notifications to be sent to multiple devices. Current deployment allows for Division of Communication and Conference Management (DCCM) to send Public Address (PA) announcements to the Baltimore outlying buildings. OEOSAS also has the ability to send messages to computers, mobile radios, scrolling displays, e-mail, phones, and the DS system.

CCS administrators and support staff user ID and password are retained for the length of time the CMS employee or contractor is assigned to CCS support.

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

Yes

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

Name

E-Mail Address

Phone Numbers

Other: Duty Station (work location), EUA User ID and passwords

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

PII is used to contact CMS employees and contractors to communicate information to them and for users of the system to gain access for system support and operations.

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

There is no secondary use for PII.

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

Executive Order 9397, the Debt Collection Improvement Act, 31 United States Code (U.S.C.) § 7701 (c)(1), and 5 U.S.C. 552a(b)(1).

5 U.S.C. Section 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.

09-70-0538 - IACS - Individuals Authorized Access to CMS Computer Services published on

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

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.

PII is not collected directly from individuals so there is no process in place to notify individuals of the collection of their personal information.

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.

PII is not collected directly from individuals so there is no process in place for individuals to opt-out of the collection or use of their PII.

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

PII is not collected directly from individuals so there is no process in place to notify individuals when major changes occur to the system.

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.

CCS maintains a trouble ticketing system using the Customer Service Inquiries tool where users can submit complaints to resolve issue regarding the system or issues with concerns over PII. The ticket will be given to the appropriate DCCM personal to review and correct the issue.

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

PII is only obtained by a transfer from the LDAP system. The PII is not editable in CCS, so it relies completely on the reviews and processes in place within the LDAP and EUA for the integrity, accuracy, availability and relevancy of the PII. Information is transferred on an annual basis from LDAP, so any changes or updates would occur at that time.

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

Administrators:

Administrators require access to the PII to update, maintain, add, and delete all system users PII within OEOSAS

Contractors:

Contractors, if they have a role as an administrator, would have the access required for the functions of that role.

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

Access to PII is based on the system user's role within CCS. The roles are customized based on the module which limits the PII data element(s) accessible to that role. The PII is also not able to be changed or amended in the system.

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.

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.

CMS employees and contractors are required to take annual Information Systems Security and Privacy Awareness training. System support staff are required to review the CCS Rules of Behavior.

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

There is no additional training.

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 National Archives and Records Administration (NARA) and CMS guidelines: General Records Schedules (GRS) 20, item 13 (Temporary. Delete when 180 days after the record keeping copy has been produced) and item 14 (Temporary. Delete when dissemination, revision or updating is completed).

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

The PII in CCS is secured administratively by the role-based access, periodic review of system user accounts and the elimination of inactive accounts.

The technical controls in place include that CCS support staff can only access the system by using their CMS issued ID. All passwords are changed every 60 days or the person will be locked out of CCS. Their accounts can only be unlocked by calling or emailing the Customer Service Inquires (CSI) hotline after verifying a person's identity. Additionally, CCS is protected by firewalls, the testing and production environments are separate and intrusion detection and intrusion prevention software is utilized.

The physical controls that are in place such as the security guards ensure that access to the building (s) are only granted to authorize individuals. The identification of everyone that enters the facility is checked and there is video monitoring of the facility.