US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/12/2016

OPDIV:

CMS

Name:

OCISO Systems Security Management

PIA Unique Identifier:
P-6394160-307599

The subject of this PIA is which of the following?
General Support System (GSS)

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?
Existing

Does the system have Security Authorization (SA)?
Yes

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

Describe in further detail any changes to the system that have occurred since the last PIA.
None

Describe the purpose of the system.
The Centers for Medicare & Medicaid Services (CMS) Office of the Chief Information Security Officer (OCISO) developed the OCISO System Security Monitoring (OSSM) system to manage the security of CMS systems across the enterprise in accordance with the Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA). OSSM comprises three unique capabilities, the CMS FISMA Controls Tracking System (CFACTS), the Continuous Monitoring Program (CMP) Continuous Monitoring Tool (CMT), and the CMS Enterprise Security Operations Center (ESOC) and its associated monitoring, response, and advanced analytics capabilities.

Describe the type of information the system will collect, maintain (store), or share.
OSSM collects security controls information, system configuration files, log files, forensic data, and

vulnerability status information. The OSSM system does not specifically target or store PII; however, PII may be inadvertently collected during a forensics investigation, or during other ESOC related monitoring of CMS systems. CFACTS collects limited POC contact information (name, work email, work phone, work organization, user IDs, passwords, and device identifiers) related to CMS employees or contractors necessary to log into OSSM, and to track and maintain CMS systems security documentation.

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

OSSM is utilized to monitor the security status of system across CMS Enterprise. The tools of OSSM work together to collect security controls information, system configuration files, log files, forensic data, and vulnerability status information. The OSSM system does not specifically target or store PII; however, PII may be inadvertently collected during a forensics investigation, or during other ESOC related monitoring of CMS systems. CFACTS collects limited POC contact information (name, work email, work phone, work organization, user IDs, passwords, and device identifiers) related to CMS employees or contractors necessary to log into OSSM, and to track and maintain CMS systems security documentation.

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

Device Identifiers

Other - Login Credentials: User IDs and passwords.

User IDs

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?

500-4,999

For what primary purpose is the PII used?

CFACTS PII (contact information and login credentials) is maintained for coordination purposes and user access only. However, there is also the potential for PII to be collected as part of a Forensic investigation.

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.

HHS Standard 2008-0006.001S
5 U.S.C. 301, Departmental Regulations

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

No

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A: CMS employee and contractor information.

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.

OSSM is not intended to collect or maintain PII, outside of official POC information and login credentials for users of the OSSM application. Based on the "Warning Banner" displayed at the time of login for any CMS system, CMS has the legal authority to collect and view this information at any time to ensure that CMS systems are not vulnerable to a security breach.

PII may be indirectly collected and may be revealed in the course of forensic investigations; however, there is no way to foresee and therefore disclose that this information will be revealed. However, standard PII breach notification procedures apply (defined in the Risk Management Handbook, Vol. II, Procedure 7.2, Incident Handling Procedure, which includes standard Breach Notification procedures.

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.

This is not applicable. Information is collected based on general system log files and is searched by automated security programs to see if CMS systems have been compromised or could be compromised. With the exception of contact information, and login credentials there is no way to foresee and therefore disclose that this information will be revealed. Additionally, an official log-on banner must be acknowledged when accessing CMS systems and warns each user that their use is subject to monitoring. OSSM is not the originator of the employee and contractor POC information, and therefore there is no ability to opt-out of the information collected.

The PII (Contact information and login credentials) is originated from a separate CMS application, which is the Enterprise User Administration (EUA), therefore there is no ability to opt-out. If the user requires access to OSSM they cannot 'opt-out' of providing their PII to EUA, as these are used to create the user within the applications.

This is not applicable. PII information is only viewed when a security breach is being investigated. Based on the "Warning Banner" displayed at the time of login for any CMS system, CMS has the legal authority to collect and view this information at any time to ensure that CMS systems are not vulnerable to a security breach. OSSM is not the originator of the employee and contractor POC information login credentials, and therefore is no ability to notify and obtain consent from these individuals when a major change occurs to the system. The PII (Contact information and login credentials) is originated from a separate CMS application, which is the Enterprise User

Administration (EUA).

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.

This is not applicable because OSSM is not designed to intentionally collect PII information. OSSM is not the originator of the employee and contractor POC information and login credentials, and therefore is no resolution process in place. The PII (Contact information and login credentials) is originated from a separate CMS application, which is the Enterprise User Administration (EUA).

Standard reporting procedures for PII breaches apply and can be found in section 2.1.4 of the Risk Management Handbook, Vol. II, Procedure 7.2, Incident Handling Procedure, which includes standard Breach Notification procedures.

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

Data collected within OSSM is not reviewed periodically unless it is required in the course of an investigation. Contact information is updated as changes occur.

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

Administrators:

Access to PII (if any) is required by Security Operations Center (SOC) personnel and forensic specialists in the course of their regular duties for incident detection, incident response, and forensic analysis

Contractors:

Access to PII (if any) is required by Security Operations Center (SOC) personnel and forensic specialists in the course of their regular duties for incident detection, incident response, and forensic analysis

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

Individuals requesting access to OSSM must sign an Account request form prior to account creation. Account request form must also be filed indicating name, email, phone number and access level needed. This form is reviewed and approved by the System information Security Officer (ISSO) prior to account creation. OSSM uses the principle of least privilege as well as a role based access control to ensure system users are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties.

Activities of all users are logged and reviewed by OSSM ISSO to identify abnormal activities if any.

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.

OSSM uses the principle of least privilege as well as a role based access control to ensure system users are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties.

Activities of all users are logged and reviewed by OSSM ISSO to identify abnormal activities if any.

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.

All users must take mandatory CMS privacy and security computer based training each year in order to maintain access to CMS systems. This training is enhanced via supplemental user awareness training and periodic security and privacy training events.

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

CMS conducts periodic security training on topics of interest throughout the year. Additionally, twice annually, specific security / privacy training is provided to CMS business owners on a range of relevant and timely security and privacy topics by CMS Security Control Oversight and Update Training (CSCOUT).

CMS employees and contractors with privileged access are required to complete role-based training and meet continuing education requirements commensurate with their role.
Other training avenues such as conferences, seminars and classroom training provided by CMS/HHS is available apart from the regular annual training.

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

No

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

The database that contains the PII is backed up by the CMS Baltimore Data Center contractor and stored off site in a secure facility. Backup tapes are rotated and destroyed in order to maintain 2 full backups at all times per NARA GRS 3.2. Item 10.

Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure continuity of security controls throughout the life of the system.

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

OSSM uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and
"need-to-access" commensurate with their assigned duties.

Activities of all users are logged and reviewed by OSSM ISSO to identify abnormal activities if any.

OSSM is hosted in a secured facility (Baltimore data center). Physical controls are in place such as security guards to ensure access to the buildings is granted to only authorize individuals. Identification of personnel is checked at the facility.

OSSM is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and National Institute of Science and
Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied.

Personally Identifiable Information (PII) in OSSM is secured administratively by ensuring that the system goes through the Assessment and Authorization (A&A) process, and all documentation is submitted to the Information Security & Privacy Group (ISPG) that supports the system and to comply with Federal Information Security Management Act (FISMA) regulations.