US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/28/2025

OPDIV:

CMS

Name:

OCISO Systems Security Management

PIA Unique Identifier:

P-6394160-307599

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Internal Flow or Collection

Describe in further detail any changes to the system that have occurred since the last PIA.

OCISO System Security Monitoring (OSSM) Splunk moved fully to Amazon Web Service (AWS). A Division of Strategic Information (DSI) program has been added to OSSM tools to leverage the Case Management Tracking System (CMTS) for case management.

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 leverages commercial-off-the-shelf (COTS) products to comprise unique monitoring capabilities such as: Continuous monitoring, Forensic and Malware, Incident management, Security Operations Center (SOC) operations, Security Engineering and Case management for insider threat capabilities.

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

OSSM collects security controls information, system configuration files, log files (through Splunk), forensic data, vulnerability status information, User ID's, passwords, and login credentials. The OSSM system does not specifically target PII, however, PII can be identified by the Master User Record (MUR) file as rolodex information. Specifically name, email, phone number, and device identifier may be inadvertently collected during a forensics investigation, insider threat investigation, or other SOC related monitoring of CMS systems. The data is stored in adherence with current regulations, memorandums, and disposal cycles as defined by the specific requirements of programs with a FedRAMP moderate system.

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, internal case management, and
vulnerability status information. The OSSM system does not specifically target or store PII; however, PII as identified by Master User Record (MUR) file as rolodex information, specifically Name, Email, Phone Number, and Device Identifier may be inadvertently collected during a forensics investigation, Insider Threat investigation, or during other SOC related monitoring of CMS systems. Splunk and CMTS are the main tools where the rolodex information will be stored and retrieved from. Limited users have access to gather data during an investigation of a security incident.

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. These login credentials are originated from a separate CMS application, which is the Enterprise User Administration (EUA) used to create the user within the application. Any PII of rolodex information to be collected is from internal employee resources, not public.

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?

10,000-49,999

For what primary purpose is the PII used?

There is the potential for PII to be collected as part of a Forensic investigation.

CDM as part of the DHS initiative portion of "who is on the network" requires PII in the form of user fields.

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

Security Operations Center (SOC) data enrichment during investigations.

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

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.

Directly from an individual about whom the information pertains

Email

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

Yes

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

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

None

Describe the procedures for accounting for disclosures.

N/A

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 is collected as part of the Master User Record (MUR) file. This will contain Active Directory rolodex information and be passed along to the HHS DHS CDM Dashboard. Standard PII breach notification procedures apply (defined in the Risk Management Handbook, Chapter 8, Incident Response, which includes standard Breach Notification procedures.)

PII may be indirectly collected and may be revealed during 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, Chapter 8, Incident Response, 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.

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 is collected as part of the Master User Record (MUR) file. This will contain Active Directory rolodex information and be passed along to the HHS DHS CDM Dashboard. Standard PII breach notification procedures apply (defined in the Risk Management Handbook, Chapter 8, Incident Response, which includes standard Breach Notification procedures.)
PII may be indirectly collected and may be revealed during 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, Chapter 8, Incident Response, which includes standard Breach Notification procedures.)

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

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 the Incident Response, Risk Management Handbook, Chapter 8, 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 during 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.

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 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 direct 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?

Yes

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

Any storage structures that contains OSSM PII are
located and backed up within secure FedRAMP
authorized cloud facilities with storage zones in
geographically disparate zones 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. For data within Splunk and passed through, the data is rolled off and removed after a rolling window of 90-days to 1-year at most unless required by m-21-31 or other agency requirements.
OSSM is not designed to provide inheritance of controls related to log and data storage. The onus of log retention and adherence to federal mandates lies upon the application, business owners, or underlying GSS services.DAA-GRS2013-00060001,DAA-GRS2013-0006-0002.

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 a Hybrid hosted in a secured facility and FedRAMP approved AWS cloud environment. Physical controls are in place such as security guards to ensure access to the buildings are 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.