US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/01/2017

OPDIV:

OS

Name:

HHS-Archer

PIA Unique Identifier:

P-9509331-023240

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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)?

No

Describe the purpose of the system.

HHS Archer is a Risk Management solution that includes an application and a database for the purpose of managing the Security Risk Management processes in compliance government mandated laws and regulations. The goal for the Archer deployment is to develop a single repository for the Health and Human Services (HHS) Office of Information Security (OIS) and its Operating Divisions (OpDivs) to aggregate data from existing information systems to drive comprehensive and informed security decisions to support operational security and risk management. Each OpDiv will maintain its own instance of Archer. Both the enterprise HHS Archer system and the OS Archer instances will consist of the following modules: Enterprise Management, Assessment & Authorization, Security Operations, Continuous Monitoring, Policy Management, and Threat Management. The OIS Archer system will serve the Office of Information Security (OIS) and its Staff Divisions.

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

The Archer system will serve as the new enterprise governance, risk, and compliance (eGRC) system for OS.

The system will also support the Department's efforts with implementing a Continuous Diagnostics and Mitigation (CDM) program. The OS Archer system will consist of six modules that will support the collection and aggregation of data.

The type of information that will reside in the Archer system will include;
An inventory of the OS systems. This will include new systems, currently operating systems, and decommissioned systems.

System Information such as certification and accreditation dates, owner and point of contact information (name , email, phone number, location), system boundaries, hardware and software, interconnections, and child applications. This will also include weakness information captured as Plan of Action & Milestone (POA&M) records.

Personally Identifiable Information (PII) data types such as privacy impact assessments (PIA) and Privacy Threshold Analysis (PTA) records for all of the systems within the OS inventory.

Scan results and vulnerabilities identified from external data sources and scanning tools.

Incident tracking through ongoing, new, and resolved incident tracking tickets and reports.

Information includes Personally identifiable information (PII) by way of collecting user credentials (email address and password) that belong to OS direct contractors and OS employees, users, etc. The user credentials are used to authenticate the user, and to determine if the user's credentials have been deleted or locked. OS Archer will maintain business contact information for HHS employees such as: name, phone number, office location, job title, name of HHS division, and email address.

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

The HHS Archer system is being designed to support the Office of Information Services (OIS) as the new enterprise governance, reporting, and compliance (eGRC) tool.
Below are the six modules that will be used to collect information with a brief description of their function.

The Enterprise Management (EM) module will support the Continuous Monitoring (CM) and Assessment and Authorization (A&A) modules. Together, they will process data from the external data sources Splunk, Forescout, BigFix, and Secure Center 5. The EM module will define the enterprise access control model to channel access based on the level within the hierarchy. The EM module will integrate people, processes, and technologies that support HHS and the OpDiv hierarchy through the management of repository HHS and OpDiv assets (applications, infrastructure, contacts, processes, and facilities).

The Assessment and Authorization (A&A) module will support design workflow frameworks as well as the implementation of a solution to secure, maintain, and demonstrate compliance for HHS and OpDiv systems. This module will define information system boundaries, assign security controls to manage risks, continuously monitor the effectiveness of the controls, and report metrics such as Federal Information Security Management Act (FISMA) reporting requirements, and provide a risk scoring model for Plans of Action and Milestones (POA&M)s. A&A will also allow users to, create and manages the Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) artifacts for the authorization package. The A&A module will allow the ability to create, assess, and authorize information systems, using National Institute of Standards and Technology (NIST) and Department of Defense (DoD) risk management framework, DoD Information Assurance Certification and Accreditation Process (DIACAP), and Federal Risk and Authorization Management Program FedRAMP.

A&A allows the ability to perform risk scoring, determine risk ratings, create and track POA&Ms, leverage controls across any number of information systems, and the ability to issue Authority to Operate (ATO) decisions for information systems and monitor and maintain ATOs through both expiration dates and risk tolerance thresholds.

The Policy module will be used to manage a repository of Federal and OpDiv specific policies, manage the training and awareness campaigns related to policies, and manage policy-related exceptions within the organization.

The Security Operations module will provide the process workflow, reporting, and program management capabilities necessary to manage a security operations center. A Security Information and Event Management (SIEM) tool such as Splunk, and other scanning tools will serve as the source of security alerts.

The Continuous Monitoring module will allow HHS to easily determine the combined impact of security metrics that rank assets by risk for faster remediation in the areas where it is needed most. The continuous monitoring modules will incorporate feeds from automated compliance monitoring tools, link compliance and vulnerability scan results with assets, provide real-time monitoring reporting of vulnerability and compliance status of information systems, incorporate feeds from automated compliance monitoring tools, and link compliance and vulnerability scan results with assets.

The Threat Management module is to reduce attack vectors, reduce weakness, understand assets and monitor activity, and minimize business impact. In order to achieve this we will monitor and manage a library of threat intelligence on issues that could impact the organization, identify and track known vulnerabilities within the organization, and manage the incident response workflow process, tracking vulnerabilities, incidents, reviews and actions items resultant from the event.

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

Mailing Address

Phone Numbers

Federal employee/contractor e-mail, mailing address, and phone number

HHS User Credentials (email address and password)

Office location (mailing address), job title and division

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

Employees

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Information in the system is used users to be able to log in and for performing the following: quarterly and annual Federal Information Security Management Act (FISMA) reporting, Plan of Actions & Milestones (POA&M) management, system PIA and self assessment completion and storage. Plan of Actions & Milestones (POA&M) management includes the tracking of system and program related security weaknesses.

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

There is no secondary use.

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

The Computer Security Act, Pub. L.100-235; and FISMA, 44 U.S.C. § 3541, et seq.

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

No

Identify the sources of PII in the system.

Other

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A

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.

Use of this federal contact information is necessary for individuals to perform their assigned duties. Individuals consent to the use of their PII in the course of employment.

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.

Use of this federal contact information is necessary for individuals to perform their assigned duties. Users do not have the option to opt-out of this as individuals consent to the use of their PII in the course of employment.

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

Any major changes to the system would be communicated to the individuals via e-mail, phone call, through administrative supervisors, and/or notices would be inserted into eGRC Archer itself.

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.

Users can report their concerns directly to the Computer Security Incident Response Center by phone or via email. In addition, users can report any suspicious use of their PII to their supervisor.

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

The data would be updated if found to be inaccurate, but periodic reviews for the PII data contained in this application because the purpose of this system is not to house accurate PII data.

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

Users:

Required for use of the system and managing their User Credentials/Profiles.

Administrators:

Required for executing the ability to manage user access.

Developers:

Required for the ability to develop reports and configures e-mail notifications

Contractors:

Only direct contractors that operate the OS Archer application on behalf of OS and use the agency's credentials have access to the system.

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

All may access who has the right to access the PII. All users of the system can see the name, phone and email of the federal employee associated with the systems in the eGRC Archer. Archer will have groups with specific access rights, and the access will be determined by management.

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.

The permissions of Archer will give the user the minimum amount of access based on roles determined by the project manager allowing the user to have access to PII items such as name, phone and email of the federal employee associated with the systems in the eGRC Archer.

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 HHS employees and direct contractors are required to take the Annual Cybersecurity Training, which includes Privacy Awareness training.

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

Additional training will be provided by direct HHS contractors with instructions on how to use the HHS Archer application.

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.

HHS Office of Information Security (OIS) is working with the Records Management office and will maintain records indefinitely until a schedule has been determined.

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

Administrative – HHS-Archer falls under the Cybersecurity Operations (CSO) contingency plan which, when activated, calls upon the Cybersecurity Operations (CSO) System Owner, HHS-Archer system administrators, and HHS security staff and contractors, to reconstitute system operations . HHS-Archer files are backed-up regularly and stored off-site. Least privileged access is granted, and user manuals are available to identify user roles and responsibilities.

Technical – Access controls are articulated through existing Department policies and procedures represented in the HHS Information Security Program Policy. Session termination is configured for a 30 minute timeout after which a session will be terminated. Remote access may be granted but only in instances in which the user is first connected to the HHS network via Virtual Private Network (VPN) encrypted tunnel. No wireless access to the application is allowed, nor are direct connections between the application and portable and mobile devices permitted.

Physical - HHS-Archer is considered an application. As such, it is dependent on the overall general support system and the environment in which that system resides for the proper implementation of physical and environmental security controls. Office of Information Security (OIS)/Cybersecurity Operations (CSO) is primarily responsible for ensuring these controls are properly implemented and regularly evaluated.

Note: web address is a hyperlink.