

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/18/2016

OPDIV:

CMS

Name:

Akamai

PIA Unique Identifier:

P-1454607-766817

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.

Contractor

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.

Not applicable

Describe the purpose of the system.

The Akamai Content Delivery Network (CDN) is a globally-distributed computing platform with over one hundred thousand servers deployed in dozens of countries, which enables businesses, government agencies, and other enterprises to extend their web presence worldwide.

Akamai Intelligent Platform (AIP) is the CDN service that CMS uses for many of its major web applications. CDN services enable CMS to deliver the large amount of publicly available information accessible to the public without a major investment in information technology infrastructure.

By leveraging the AIP's ability to resize to a large volume based on user need and the capability to provide a stored or readily available website for faster served content, CMS is able to meet high internet traffic demand, and at the same time thwart malicious traffic by having the security perimeter at Akamai's Web Application Firewall (WAF).

CMS also utilizes is the Akamai Luna Control Center (Luna). It is an online command and control website, which provides CMS customers with near real time Security Monitor and Trend Reporting on information security attacks.

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

Akamai provides CMS administrators and security personnel access to the Luna Control Center, an online command and control website that provides real-time reports on internet activity and information/network security attacks. Luna collects and stores users' login credentials. The system user's name, phone number and email are collected for user registration purposes and a user ID and password are used to access the system.

If CMS needs more detailed visibility and information about the attack traffic, the service can be configured to send logs directly to them for analysis. Akamai also has the ability to collect, store and share Internet Protocol (IP) addresses.

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

CMS utilizes the Akamai CDN intelligent platform to manage the large volume of publically available information on many of their major applications. CMS also uses the Akamai Luna Control Center, an online command and control website to manage real-time security monitoring of the internet traffic to CMS websites.

CDN services enable CMS to deliver the large amount of publically available information accessible to the public without a major investment in information technology infrastructure. By leveraging the AIP's ability to resize to a large volume based on user need and the capability to provide a stored or readily available website for faster served content, CMS is able to meet high internet traffic demand, and at the same time thwart malicious traffic by having the security perimeter at Akamai's Web Application Firewall (WAF).

The Luna Control Center has the ability to hide the true Internet Protocol (IP) address of a server, called web proxy/caching. CMS uses the web proxy/caching option where Akamai hosts CMS static web application content through their secure network. Akamai uses the actual application server IP address in order to host the application for CMS. This IP is not exposed to the general public. The public users see an Akamai created IP and static website. This will prevent CMS servers from getting attacked as the true IP addresses are unknown to end users.

Luna collects and stores users' login credentials. The system user's name, phone number and email are collected for user registration purposes and a user ID and password are used to access the system. If CMS needs more detailed visibility and information about the attack traffic, the service can be configured to send logs directly to them for analysis.

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 - User ID and password, IP addresses

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

Employees

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

PII is used to identify and authenticate users within the system.

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

Not applicable

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

5 USC § 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

In-Person

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable

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.

The information is used for registration and individuals would be notified by CMS that their personal information will be collected; individuals are notified by email to identify that they are registered and to change their login password.

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.

Collecting login credentials (user ID and password) is essential for access to Akamai. It is necessary to identify the user for identification and authentication to the system. There is no option to object to the information collection for this reason.

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

The process to notify individuals of major changes to the Akamai system would occur through the Akamai Luna Control Portal log-in screen and the posted "Akamai Portal Terms of Use." Consent to changes to the system is not provided because the CMS users are essentially 'customers' of Akamai.

The Luna Portal-specific privacy policies and terms and conditions are a link on the portal are located at this URL:

<https://www.akamai.com/us/en/privacy-policies/portal-terms.jsp>

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.

Within the Akamai Privacy Statement posted on the website is a section "Contact Akamai" that provides the methods by which a user may contact Akamai, if the individual has any concerns about the PII that Akamai collects and stores. The individual would contact the Privacy Department at either privacypolicy@akamai.com or by mail to

Akamai Technologies, Inc. 150 Broadway Cambridge, MA 02142 Attention: Chief Privacy Officer

The Akamai Privacy Statement:

<https://www.akamai.com/us/en/privacy-policies/privacy-statement-for-akamai-sites.jsp>

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

Because Akamai controls the access to their portal, CMS does not have a process to review the PII within it for integrity. The Akamai Luna Portal allows registered/authorized users to manage their user ID and/or password. This allows the authorized user to manage the accuracy and integrity of their account information. Additionally, CMS Akamai system administrators periodically review the list of authorized users for relevancy and availability to supply to Akamai to allow the users to create user accounts.

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

Administrators:

Administrators have access to PII as required to maintain and manage the user accounts.

Contractors:

CMS direct contractors, in their role as an administrator, would have access to PII as required to maintain and manage user accounts.

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

Akamai uses role-based access controls to ensure that administrators are granted access on a 'least privilege' basis commensurate with their assigned duties. System administrators determine the role-based access rights of any other users.

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.

Akamai uses role-based access controls to ensure that administrators are granted access on a 'least privilege' basis commensurate with their assigned duties. Job codes are assigned in order to grant appropriate levels of access.

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 CMS employees and direct contractors are required to take the annual Security and Privacy Awareness training, which includes an examination at the end to certify completion.

Akamai has a code of ethics to which all users are required to abide, which includes safeguarding sensitive information:

<https://www.akamai.com/us/en/privacy-policies/code-of-ethics.jsp>

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

Not applicable.

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.

Akamai follows the National Archives and Records Administration (NARA) record GRS 3.2, Item 30 and 31 which set a minimum length of time for retention as 'when business use ceases' and a maximum length of retention of 6 years, after which destruction is allowable if there is no further need for the records.

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

The administrative controls in place are that access to Akamai is highly restricted to a small set of users, role-based access for users and the users must be pre-approved by CMS in order to access the Luna Control Center.

The technical controls in place include encrypted log-on procedures, two-factor authentication of users for identification and authentication and system administrators review user accounts at least semi-annually. Additionally, activities of all users including system administrators are logged and reviewed by the Akamai Information System Security Officer (ISSO).

The physical controls in place include servers located in a secured data center with surveillance, locked rooms, and a separate network operations center, and security guards and badging of personnel for access.