US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/21/2022

OPDIV:

ACF

Name:

Next Generation Secure Cloud (NGSC)

PIA Unique Identifier:

P-4982088-658586

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

Is this a FISMA-Reportable system?

No

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

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

Describe the purpose of the system.

Administration for Children and Families Office of Chief Information Officer (ACF OCIO) currently supports a cloud based General Support System (GSS) in the Amazon Web Services (AWS) commercial cloud. This legacy environment is not built to support the functional, operational, and security requirements needed to properly manage and secure modern applications. This capability gap includes but is not limited to network and data segmentation, event and incident detection, and the ability to support agile and scalable systems for the various ACF missions. These deficiencies put ACF data at risk of denial of availability or even loss through exfiltration or technical failure.

The Next Generation Secure Cloud (NGSC) Cloud General Support System will be an interconnected and interoperable set of information resources centered on levering a commercial cloud infrastructure. This will provide the Administration for Children and Families (ACF) a more agile and secure environment for developing, testing, and hosting software applications.

The scope of the Next Generation Secure Cloud (NGSC) project is to design, implement, and move

to initial operations a minimal viable cloud environment, including all internal and external networks, and to create a single commercial cloud environment to support not only production applications, but development, test, and staging for software enhancements and new application development. The NGSC will function as a General Support System (GSS) environment to provide information resources under the same direct management control that share common functionality across all production, development, test, and staging environments. This project will serve to “re-home” the applications from the existing AWS environment to this new environment. This will establish a secure environment in which to host ACF applications that meet or exceed security guidelines and ensure that we are implementing and leveraging our security and operational tools in a cost-effective manner.

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

The AWS management console controls the provisioning of servers and services across the environment. The information collected and maintained within the NGSC GSS includes system log files, an inventory of all NGSC GSS servers, and relevant server attributes such as server names, Internet protocol (IP) addresses, availability zone, and resource allocation. Applications running on the GSS collect the following the types of data, respectively:
McAfee anti-virus solution and AlertLogic Intrusion Detection System (IDS) collect and maintain attributes related to information security that are used to detect potential threats.
Nagios collects server and network monitoring baseline attributes such as Central Processing Unit (CPU) usage, disk space, and memory usage. Monitoring attributes can be customized to gather additional information such as website monitoring details or specific application system monitoring details.
Splunk collects and maintains information to support security incident and event management (SIEM) such as IP addresses, Fully Qualified Domain Names (FQDNs), NetBIOS names, and system or application log data.
Nessus conducts vulnerability scans which includes data elements such as IP addresses, FQDNs, NetBIOS names, hardware types, and software versions.

NGSC GSS also collects and maintains account management information for privileged users on the ACF OCIO Operations Support contract and federal staff privileged users. All NGSC GSS privileged user accounts include the user first and last name, e-mail address, user role(s), and user credentials (username and password). User accounts reserved for federal staff include a root user account granted to the ACF CIO and an AWS Cloudwatch account which provides billing account information. Direct contractors are granted Super Administrator, Administrator, or Database Administrator accounts.

Additionally, the GSS operates a secure file transfer protocol (SFTP) server that ACF programs may leverage for application deployments and data transfer projects. The OCIO Operations team controls the access and process for the use of the SFTP server and all requests adhere to the OCIO change management process which requires leadership approval. Any given project using the SFTP server may involve personally identifiable information (PII) within data files, which is why an OCIO standard operating procedure is followed to remove both the data files and the accounts provisioned at the conclusion of the effort.

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

The NGSC GSS provides Platform as a service (PaaS) and Infrastructure as a service (IaaS) functions to support the hosting of ACF mission applications. The information collected within the GSS, (user first and last name, e-mail address, user role(s), and user credentials) is used to support the operations and maintenance of the environment and hosted applications. All applications hosted within the GSS that collect, maintain, or share information (which may include personally identifiable

information, PII) are covered by their own privacy impact assessment (PIA).

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

Yes

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

User roles

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

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

The primary purpose of the PII is to establish and maintain privileged user accounts to support GSS and application operations and maintenance.

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

There is no secondary use of the PII.

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.

Identify the OMB information collection approval number and expiration date

Not applicable (N/A). Information collected from federal employees is exempt from the Paperwork Reduction Act if the information collection falls within their work duties; information collection is similarly exempt for contractors if the collection is only for basic contact 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.

Privileged users of the NGSC GSS are implicitly made aware of their PII collection because of the account management process. Account requests are generated for users on behalf of their manager and submitted via email to the ACF CIO or Deputy CIO. Requests are provided in the form of an updated workbook detailing the username, credentials, and requested roles and privileges. Following the request review, the CIO or Deputy CIO will notify the manager and the NGSC GSS Lead engineer confirming the creation of their account.

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.

The individuals requiring an account in the environment cannot opt-out of the collection due to job or project responsibilities.

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

Users of the NGSC GSS are notified directly by email in the event of major system changes.

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.

Individuals concerned with the accuracy of their account information are directed to notify the NGSC GSS Security Lead Engineer and ACF Incident Response Team (IRT) via email. The Engineer will elevate the issue to the ACF Deputy CIO for review and approval to remediate their concern. Individuals concerned that their PII has been compromised must notify their supervisor and the ACF Incident Response Team (IRT) for investigation.

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 integrity for the NGSC GSS is maintained by limiting access to the system to users approved for access. All user account requests to add, remove, or modify, are reviewed by the senior cloud architect. The review includes verification of user account name and contact information, role, and access requirements for the individual. Following the review, a request to approve the changes is sent to the System Owner and/or the Chief Information Officer (CIO) for approval. Upon approval, the changes are performed and are documented in a privileged account workbook.

Data relevancy and accuracy for NGSC GSS is maintained by conducting routine reviews of stale or inactive accounts every 30 days. The workbook is reviewed by the system owner at least every 90 days. Additionally, NGSC GSS data follows specific retention and destruction schedules in accordance with National Archives and Records Administration General Records Schedules (NARA GRS) disposition authorities.

Data availability is established through ACF and AWS contractual agreement. The Service Level Agreement states that AWS will provide a monthly up-time percentage of at least 99.9%.

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.

There are formal account request procedures followed for roles that access PII. These request procedures identify the specific role, permissions that the account will be granted, and the specific server and/or application. The roles and permissions granted are identified by the technical architect lead and each account request form is then reviewed and approved by the Contracting Officer's Representative (COR) or Government Technical Manager prior to account creation.

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 roles and permissions granted limit the level of access a particular account will have. Individuals with super administrator access have elevated permissions to manage accounts and access all servers within the environment. Access is limited to only the personnel that support the GSS from an infrastructure perspective or support an application hosted within the GSS.

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 personnel including both direct contractors and government personnel are required to participate in the ACF annual security compliance training and privacy training. Additionally, account holders are required to complete the Health and Human Services (HHS) Rules of Behavior (RoB), including the privileged user addendum.

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

All privileged users supporting this GSS are required to complete the privileged users training annually.

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.

The information collected and maintained in support of the operations and maintenance of the GSS will be kept in accordance with the following NARA GRS disposition authorities:
Schedule 3.2, item 031, DAA-GRS-2013-0006-0004 for system access records in which records are destroyed 6 years after a password is altered or a user account is terminated, but longer retention is authorized if required for business use.
Schedule 3.2, item 040, DAA-GRS-2013-0006-0005 for backup records in which records are destroyed when superseded by a full backup, or when no longer needed for system restoration, whichever is later.
Schedule 3.2, item 041, DAA-GRS-2013-0006-0006 for backup records in which the records are destroyed when a second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.
Schedule 3.2, item 051, DAA-GRS-2013-0006-0008 for backups of master files and databases in which records are destroyed immediately after the identical records have been deleted or replaced by a subsequent backup file or longer retention is authorized if required for business use.

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

The GSS has a shared responsibility model for the administrative, technical, and physical safeguards. Part of the responsibility lies with the operator, AWS, and the other part is implemented and managed by the OCIO infrastructure team.

The physical controls are provided by AWS and include fire detection and suppression requirement, uninterruptible power supply (UPS) units, climate control, preventative maintenance, video surveillance and security staff, and a thorough access control policy.

The technical controls are shared responsibility and include a fault-tolerant design to support high availability, network access control lists (NACLs), security groups, and route tables.

The administrative controls managed by ACF include processes and procedures for account and change management, training requirements, and role-based access control (RBAC).