US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/18/2022

OPDIV:

ACF

Name:

Child Welfare Information Gateway - NextGen Gateway (CWIG NGG) General Support System (GSS)

PIA Unique Identifier:

P-7115608-771365

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.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The Child Welfare Information Gateway – NextGen Gateway (CWIG NGG) General Support System (GSS) will consolidate CWIG's legacy systems under one roof into a hybrid cloud environment consisting of Amazon Web Services (AWS) and ServiceNow (SNOW). This centralized platform is FedRAMP-approved and will better align CWIG's IT systems with federal security requirements and mandates. Legacy systems will be modernized and migrated incrementally into the new environment. CWIG will leverage SNOW's many out-of-the-box functions to simplify production and management of CWIG's IT systems. A GSS will be established that integrates and extends the foundational AWS cloud infrastructure with SNOW.

The GSS will reduce the agency overhead of ATOs for the migrated applications under CWIG because application specific Authorization to Operates (ATOs) will inherit CWIG NGG GSS system security controls, as applicable, thus simplifying the process. The resulting system will provide a cohesive, secure, and streamlined system with increased transparency for the Office of the Chief

Information Officer (OCIO).

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

The GSS infrastructure, which includes AWS and SNOW, will store all code, scripts, logs, and automatic builds necessary to deploy and maintain the CWIG NGG GSS. The GSS will also collect administrative user's first name, last name, and ACF email address to login to each platform. No information is shared outside of the CWIG NGG GSS.

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

The information collected and stored within the GSS is used to support the operations and maintenance of the environment and hosted applications. The GSS will collect and store application code, scripts which run automated back-end jobs, audit logs which capture all actions taken by users in the environment, and automatic builds that are used for deployments. For authentication purposes, administrators must provide their first name, last name, and ACF email address. This data is not shared outside of the CWIG NGG GSS. All applications hosted within the GSS that collect, maintain, or share information (which may include personally identifiable information, 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.

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?

Establishing and maintaining privileged user accounts to support GSS and application operations and maintenance.

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

There are no secondary uses 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, OMB information collection approval numbers is not needed for CWIG NGG GSS as this is an infrastructure only and does not have any application interfaces or collect any information from any individuals or from any source.

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.

Individuals are notified their personal information is collected when they join the CWIG team and provide their personal information to HR and the Ops division.

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; however, their concerns can be shared with the Ops division/HR responsible for handling documentation.

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

If there is a change, the CWIG team will use a shared platform such as a SharePoint portal or email to disseminate information between the project manager and system administrators. The project manager informs the appropriate system administrator on pending changes to their system via email or SharePoint. The change is either accepted or they will no longer have access to that system in order to prevent disclosure.

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.

The CWIG team will follow an established process in which if Personally Identifiable Information (PII) has been stolen or obtained inappropriately, an incident reporting procedure will be set up to inform all employees on contacting the help desk and reporting the problem up. Every user of the system will be responsible for monitoring for suspicious behavior and can follow a process to inform the help desk or incident response team on the details. If system users believe that their information has

been inappropriately obtained, used, or disclosed, they may report to the Project Manager for appropriate review and escalation for investigation as needed.

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 CWIG team assesses the CWIG NGG GSS system environment for vulnerabilities or other security issues that would impact availability, integrity, and confidentiality of information in the system and ensure they are identified on time. Periodically, for accounts management, the CWIG team is expected to review users to determine whether their access should stay active or get deactivated. To maintain the system's integrity, availability, accuracy, and relevancy of its information, the CWIG team looks at whose information needs to be deleted from the system and make updates where required based on the latest system changes. The CWIG team also defines the minimum security and privacy controls (in Appendix K of the System Security Plan (SSP) to address concerns related to the privacy impacts on the system and users.

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.

The project manager and/or system owner assigns user roles/responsibilities and determines who will need access to the PII. The roles that may need access to PII include the System Admin and Account Manager. These accounts are approved by the Federal COR for the project. Access is assigned on a need-to-know basis as well as least privilege. A user will have to be set up or flagged as active in order to gain access to the system and its PII.

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.

Access is assigned on a need-to-know basis. This access is provided off a role-based authorization method and users are granted access to the information only at the minimum amount needed to accomplish their jobs.

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.

The team also takes HHS/ACF required annual Computer Security Awareness Training, Privacy Awareness Training, and Records Management Training.

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

All CWIG team members are provided security awareness and training by the contractor company that are specific to their positions on the project. Team members also receive training on incident response and disaster recovery.

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.

Once the system is covered by a records retention schedule, retention guidelines will be established with system owners to satisfy NARA requirements. Development of records retention policies are currently in progress and will be submitted to NARA for approval on proposed record schedules.

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

Administrative: Access to PII is assigned on a need-to-know basis. This access is provided off a role-based authorization method and users are granted access to the information only at the minimum amount needed to accomplish their jobs.

Technical: There will be no PII captured in the GSS until a user is authenticated. Once the authentication is completed, the PII captured will be secured by using Two-Factor Authentication which is covered under the technical control of identification and authentication - IA-02(01). The privileged accounts will be audited to ensure integrity of PII in accordance with the Access control policy - AC-06.

Physical: All physical controls are inherited from AWS and ServiceNow as the CWIG NGG GSS is a fully cloud based solution. Both Cloud Service Providers (CSPs) have undergone FedRAMP authorization assessments to ensure they have appropriate physical controls to protect the PII stored in the CWIG NGG GSS.