US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2026

OPDIV:

ACF

Name:

Child Welfare Outcomes (CWO)

PIA Unique Identifier:

P-3438814-668213

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

Yes

Identify the operator.

Contractor

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.

The U.S. Department of Health and Human Services (HHS) prepares a series of annual reports. HHS is responsible for monitoring programs and services that address the needs of children and families who engage with public child welfare systems. The Children’s Bureau (CB) carries out these responsibilities, in collaboration with Information Gateway, and prepares the Child Welfare Outcomes (CWO) reports for Congress. The CWO portal enables State and Region government agency users to log in and review their annual Child Welfare Outcomes data and upload a formal comment.

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

The CWO portal stores and displays Child Welfare Outcomes comprehensive data for each State related to Child Population, Child Maltreatment, Foster Care and Adoption for a given year. Personally Identifiable Information (PII) such as name and work email address are collected for user authentication. This data is never shared outside of the CWO / Amazon Web Services (AWS) Cognito systems.

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

The Child Welfare Outcomes (CWO) application enables State and Regional Agency Users to review annual state data related to child population, maltreatment, foster care, and adoption outcomes, and to upload formal comments. Administrator Users at the Children's Bureau (CB) can view dashboards, monitor submissions, and download formal comments for Congressional reporting. CWO operates within the Child Welfare Information Gateway NextGen Gateway General Support System (CWIG NGG GSS) environment (AWS, FedRAMP Moderate).

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
User credentials

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

Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

To establish and maintain privileged user accounts to access the CWO portal via AWS Cognito and for email subscription's purposes

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

N/A

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

5 USC 301, Department Regulation.

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
Online

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.

State Agency Directors provide their names and email addresses when they subscribe to receive

emails from the CWO State Contacts List, managed by CB. Privacy information remains accessible to the users through the ACF Privacy Policy link which is present in the footer on the CWO State Data Portal home page. Individuals are informed during registration that their information will be used only for authentication.

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.

No opt-out available; user access requires registration. Government agency users who require access to the CWO portal to review State outcomes data and provide formal comment must agree to the collection of their PII (work email address) for the sole purpose of user authentication. This data is never shared outside of the CWO / AWS Cognito systems.

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

Material changes are communicated through the childwelfare.gov Privacy Policy update and CB stakeholder emails.

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.

If a user has a concern about the use of their work email address as their username, they can contact the Child Welfare Outcomes program team, via the cwoutcomes@childwelfare.gov email address provided on the CWO State Portal home page, to raise any concerns they may have. The CWIG Staff follows the ACF Incident Response 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.

Since the PII collected is limited to authentication information (work email address):
Integrity: User account information is protected from unauthorized modification through access controls that limit system administration to authorized Super Administrator users only.

Availability: Authentication data is maintained in a secure database with appropriate backup procedures to ensure it is available when needed for system access.

Accuracy: User information is verified at the time of account creation. Users can contact the Child Welfare Information Gateway program team if they need to update their information.

Relevancy: User accounts are reviewed regularly as part of the off-boarding process. When an individual no longer requires access to the system, their account information is removed entirely, ensuring only relevant user information is maintained.

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.

Access to the CWO usernames is limited to AWS Cognito system administrators. User accounts are created, and roles are assigned at the request of the Children’s Bureau.

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.

Only the ICF CWO Super Administrator roles can access the username (work email address) of system users for the sole purpose of user account management and authentication.

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.

Training is provided for all personnel, including:

ACF Cybersecurity awareness training (CSAT) covering PII handling best practices. Specialized training for administrators and developers on secure data management. And periodic refresher courses to address evolving privacy policies and security risks.

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

All privileged users with system administration responsibilities are required to take mandatory annual compliance training including:
-Cybersecurity Awareness Training (CSAT), which includes Privacy 101
-Role-based Security Training
-Global Data Protection and ePrivacy
-Code of Business Ethics & Conduct
-Protecting Intellectual Property

State and Region agency users of the system are not required to complete formal training as they do not have elevated system privileges.

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.

GRS 3.1: General Technology Management Records
Disposition Authority: DAA-GRS-2013-0005-0004 (Item 20)
Disposition Instructions: Temporary, destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

GRS 3.2: Information Systems Security Records
Disposition Authority: DAA-GRS-2013-0006-0003 (Item 30)
Disposition Instructions: Temporary, destroy when business use ceases.

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

Administrative Controls: The system employs robust administrative safeguards to protect user PII. Access management is strictly controlled through a formal authorization process that requires management approval before accounts are created. Role-based access controls (RBAC) are implemented to ensure users can only access information necessary for their job functions, with Super Administrator privileges limited to designated ICF personnel. All system users must complete mandatory security and privacy training, including ACF Cybersecurity awareness training covering PII handling best practices. Regular compliance reviews and account audits are conducted to verify adherence to security policies, with particular attention to prompt removal of access when no longer required through a documented off-boarding process.

Technical Controls: The CWO portal implements comprehensive technical safeguards within a secure cloud infrastructure built on zero-trust architecture principles. All authentication data is protected using industry-standard encryption both in transit and at rest. The system requires multi-

factor authentication for all user access, ensuring that username and password combinations alone are insufficient for system entry. Access attempts are logged and monitored for suspicious activity, with automated alerts for potential security incidents. System sessions automatically time out after periods of inactivity to prevent unauthorized access to unattended workstations. Regular security scans and vulnerability assessments are performed to identify and remediate potential weaknesses in the system's technical controls. Encryption in transit and at rest (TLS 1.2, AWS KMS), MFA for all users, logging via AWS CloudWatch, and session timeout enforcement.

Physical Controls: Physical security is maintained through hosting within government-approved cloud environments that meet FedRAMP security requirements. These facilities implement strict physical access controls including biometric verification, security personnel, video surveillance, and visitor management systems. Environmental controls such as fire suppression, climate regulation, and backup power systems protect against physical threats to data availability. All system hardware is maintained in secured data centers with comprehensive disaster recovery capabilities. The cloud service providers maintain compliance with federal security standards and undergo regular third-party audits to verify the effectiveness of physical security measures. FedRAMP-authorized AWS data centers with biometric access, video surveillance, and environmental controls.

Identify the publicly-available URL:

https://cwoutcomes.acf.hhs.gov/cwoutcomes

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Other technologies that do not collect PII:

- AWS CloudFront Access Logs
- Google Analytics (aggregated metrics only)

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes