US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/03/2016

OPDIV:

ACF

Name:

DBRM Personnel

PIA Unique Identifier:

P-5178253-538965

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?

No

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 mission of the U.S. Department of Health and Human Services (HHS) is to enhance the health and well-being of Americans by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services. As an Operating Division (OPDIV) of HHS, the mission of the Administration for Children and Families (ACF) is to promote the economic and social well-being of children, youth, families, and communities, focusing particular attention on vulnerable populations such as children in low-income families, refugees, and Native Americans. ACF directly supports HHS' Strategic Goal 3: Advance the Health, Safety and Well-Being of the American People, further supporting the three Secretary's Priorities: 1) Put Children and Youth on the Path for Successful Futures, 2) Promote Early Childhood Health and Development, and 3) Ensure Program Integrity, Accountability and Transparency.

The Office of Child Support Enforcement (OCSE) is the federal government agency that oversees the national child support program. We help child support agencies in states and tribes develop, manage and operate their programs effectively and according to federal law, through partnering with state, tribal and local child support agencies and others to encourage parental responsibility so thatchildren receive financial, emotional, and medical support from both parents, even when they live in separate households. We promote effective child support enforcement tools coupled with family-centered customer service. Within ACF the following strategic goals was identified, “People Are Our Greatest Resource: ACF will establish a work environment and culture that people will believe in and thrive in to achieve mission success. Establish leadership focused on defined and attainable goals, objectives and approaches that people will believe, trust and follow.

Within the mission functions of OCSE is a goal to attract a highly skilled workforce and establish a culture that has a positive impact on the efforts and productivity of OCSE staff. The OCSE personnel management group in meeting this mission goal and objective must ensure continued acquisition, development, support and monitoring of OCSE staff. OCSE established the Division of Business and Resource Management (DBRM) Personnel system to manage personnel records for the OCSE personnel management group.

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

The DBRM Personnel system collects, maintains (stores) and shares data including first and last name, email address, phone number, education records, date of birth, location (mailing address), employee status (Grade Level), salary, user credentials (username and password), and training records on OCSE employees. The OCSE Personnel management group uses the system to maintain records on the employees, and does not share data with other organizations. User credentials are maintained only for HHS employees and direct contractors that required system accounts to fulfill their job duties.

This data is directly entered into the system by OCSE staff and is not derived from interface or upload from another information technology system or database. The system does not interface, integrate, or share data with any other information technology system or databases.

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

The DBRM Personnel system collects, maintains (stores) and shares data (Information includes name, email address, phone number, education records, date of birth, location (mailing address), employee status (Grade Level), Salary, and Training) on OCSE employees and the OCSE Personnel management group uses the system to maintain records on the employees, and does not share data with other organizations. The information and PII is collected to track, monitor, oversee and manage employee records and information and for the purpose of employee identification.

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

Yes

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

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Education Records

Employment Status

User Credentials

Salary

Training Information

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?

The primary purpose for the DBRM Personnel system collecting PII (name, email address, phone number, education records, date of birth, location (mailing address), employee status (Grade Level), salary, user credentials, and training) is to track, monitor, oversee and manage employee records and information and for the purpose of employee identification.

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

Not Applicable (N/A)

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?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-90-0001 Telephone Directory/Locator System

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not Applicable (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.

There is no process in place to notify individuals that their personal information is being collected. The individual provides the information when they apply for employment at OCSE which is a voluntarily act. After a user requests access to the DBRM Personnel system, an email approval request is sent to the manager. After official written approval, the administrator creates the user account then notifies the user via email or phone to let them know that a user account has been created with their information.

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.

Individuals cannot opt out of the collection of their information because OCSE collects the following PII data from end users for access control: name, e-mail address, location (mailing address) and phone number and is based upon consent of the end users for creating an end user account.

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

DBRM Personnel system collects the following PII data from end users for access control: name, e-mail address, location (mailing address) and phone number and is based upon consent of the end users for creating an end user account. End users are notified by the system administrator and their consent is obtained from the individuals whose PII is in the DBRM Personnel system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection)

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.

DBRM Personnel system collects the following PII data from end users for access control: name, e-mail address, location (mailing address) and phone number and is based upon consent of the end users for creating an end user account. There are processes 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. System users contact the system program manager or system administrator with concerns about their user account. Users can either contact via email by sending a message to an OCSE mailbox or by submitting a ticket on the OCSE SharePoint site. At that time, the program manager and system administrator will work together to evaluate the user's concern, review the logs to determine if there is indeed an issue, and then work to resolve any concerns related to inappropriately used data or incorrect data. Once that is done, the user will be contacted and updated on the issue via email or phone.

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 need and requirement for data integrity, availability, accuracy, and relevancy will be immediately apparent to the system user and can be rectified by contacting the system program manager or system help desk with concerns about their user account. Also should the end user require an update to the PII data in the end user account (e.g. name, email address, location (mailing address) or phone number change) the end user can contact the system program manager or system help desk with concerns about their user account.

When a user leaves OCSE and no longer needs a user account, a written request to remove the user is sent out to the system administrator after approval from a manager. The administrator removes the user account and all related PII data.

There is a new process in place to review the list of users for Integrity, Availability, Accuracy and Relevancy. The user list is reviewed by the project manager or system owner to determine if any user data/access needs to be updated or removed. The manager then notifies the administrator of the updates needed to the OCSE Directory user list. This process takes place on a annual basis.

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

Users:

Personnel Management

Administrators:

Need access to resolve issues with the system

Contractors:

The administrators are direct contractors

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

End user accounts are requested through the program office system owner/program manager who reviews, authorizes and approves the creation of the end user account based upon the individual end user's roles and responsibilities associated with the OCSE program. The authorized and approved account creation request is submitted to the DBRM Personnel system, system administrator who creates the individual account and notifies the end user of the authorized, approved, and created account. The end user initially logs on, provides appropriate information to authenticate himself/herself enabling account access.

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.

End user accounts are requested through the program office system owner/program manager who reviews, authorizes and approves the creation of the end user account based upon the individual end user's roles and responsibilities associated with the OCSE program. The authorized and approved account creation request is submitted to the DBRM Personnel system, system administrator who creates the individual account and notifies the end user of the authorized, approved, and created account. The end user initially logs on, provides appropriate information to authenticate himself/herself enabling account 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 Department users to include federal employees, contractors, and other system users must review and sign an acknowledge statement of the HHS Rules of Behavior (RoB). This acknowledgment must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. All users of Privileged User accounts for Department information technology resources must read these standards and sign the accompanying acknowledgment form in addition to the HHS RoB before accessing Department data/information, systems, and/or networks in a privileged role. DBRM Personnel system end users are required to complete the following:

Annual HHS Information Systems Security Awareness Training;

Annual HHS Privacy Training; and

Reading the Rules of Behavior for Use of HHS Information Resources and signing the accompanying acknowledgment.

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

Cursory end user training and documentation is provided DBRM Personnel system co-workers. No specific or periodic, annual or refresher training is provided. There is no system-specific training for PII.

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.

OCSE is in communications with the ACF Records Manager to determine the specific National Archives and Records Administration (NARA) retention schedule. All records will be retained until a determination is made as to the final records disposition schedule. Once established the records will be disposition consistent with the records disposition schedule.

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

PII is secured using the following:

Administrative controls, including but not limited to:
System security plan (SSP)
File backup/archive

Technical Controls:
User Identification and Authorization
Passwords
Firewalls at hosting site
Monitoring and Control scans

Physical controls
The system servers are hosted in a secure data center and can be physically accessed by only the authorized infrastructure staff from ACF/HHS can access. Enforcement of established physical security capabilities (management walk-throughs and assessment of security locks, doors, desks, storage materials, Security Guards employing access controls to individuals requesting facility access:

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. All physical access to data centers by employees is logged and audited routinely. Secured and limited access facilities: data center access and information to employees and contractors who have a legitimate business need for such privileges.
When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee.