US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/18/2025

OPDIV:

ACF

Name:

National Directory of New Hires

PIA Unique Identifier:

P-6384563-016353

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.

Agency

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.

No significant changes have been made to the National Directory of New Hires (NDNH).

Describe the purpose of the system.

The NDNH is a national repository of employment information. It accepts New Hire and Quarterly Wage (QW) information from states, U.S. territories (Guam, Puerto Rico, and the Virgin Islands), and federal agencies. The NDNH also receives Unemployment Compensation Insurance (UI) benefit information from all states and two U.S. territories (Puerto Rico and the Virgin Islands).

The NDNH works with other systems in the Federal Parent Locator Service (FPLS). Its primary role is to help state child support agencies locate noncustodial parents, alleged fathers, and custodial parents. This tool helps establish paternity, set child support obligations, and modify and enforce child support orders. It also provides support in the resolution of custody and visitation issues.
The Multi-State Employer Registry is a sub-system of the NDNH. According to section 453(i)(4) of

the Social Security Act (42 U.S.C. § 653(i)(4)) the Secretary of Health and Human Services must keep a list of multistate employers who choose to report to one state. The list also includes which state the employer is reporting to. The Office of Child Support Services (OCSS) sends this list to each State Directory of New Hires (SDNH) every month.

OCSS may use NDNH data to create de-identified or aggregated datasets for reporting. These datasets may be used by the Department of Health and Human Services (HHS) or other agencies for analysis.

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

The NDNH system collects various types of personally identifiable information (PII) related to employment, wages, and unemployment compensation. This data is collected from state and federal agencies, as well as U.S. territories, to locate child support obligors, verify eligibility for certain programs, and support the administration of employment security and workers' compensation programs. Information collected includes:
Newly Hired Employee Records from SDNHs: Employee first and last name, mailing address, date of hire, Social Security Number (SSN), date of birth (optional), employer name, employer address, and Federal Employer Identification Number (FEIN). [Social Security Act, 42 U.S.C. § 653a(g)(2)(A)].

Newly Hired Employee Records from Federal Agencies: Employee first and last name, mailing address, date of hire, SSN, date of birth (optional), employer name, employer address, and FEIN. [Social Security Act, 42 U.S.C. § 653a(b)(1)(C)].
Wage and UI Records from State Workforce Agencies (SWA): Employee/Claimant SSN, employee/claimant name, employee/claimant address, wage/claimant benefit amount, employer FEIN (for wages), and reporting period. [Social Security Act, 42 U.S.C. § 653a(g)(2)(B)].

Wage Records from Federal Agencies: Wage information provided by federal departments or agencies. [Social Security Act, 42 U.S.C. § 653(n)].

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

The New Hire File contains information on all newly hired employees as reported by employers to each SDNH. Federal agencies report directly to the NDNH. Employers are required to report: employee name, employee SSN, employee mailing address, employer name, FEIN, employer address, and date of hire. Note that "New Hire" refers to the type of information; the information may not necessarily be new to the system.

The QW File contains quarterly wage information on individual employees from SWA and federal agency records. The NDNH
receives employee name (if collected by the state), employee SSN, employee wage amount, reporting period (calendar quarter in which wages were paid), employer name, FEIN, employer address, and employer optional address.

The UI file contains UI information on individuals who received or applied for unemployment benefits, as reported by SWAs.
States transmit the following UI data elements to the NDNH: claimant name, claimant SSN, claimant mailing address, claimant benefit amount (gross amount before any deductions), and reporting period (calendar quarter in which the UI claim was filed).

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

Yes

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

Social Security Number
Date of Birth
Name
Mailing Address
Military Status
Employment Status

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

Employees
Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose of PII collected by the NDNH is to help states locate parents or relatives and provide child support services. The data also helps authorized federal and state agencies determine or verify applicant eligibility for federal or state benefit programs, and to recover benefits or debts related to these programs.

State Child Support (CS) agencies use this information to find noncustodial parents, establish paternity, and identify which state has legal authority to establish, change, or enforce child support orders.

Federal law permits sharing specific types of information with authorized entities for clearly defined purposes. The information is shared with CS agencies, courts with the authority to issue child support orders, and resident parents, legal guardians, attorneys, or agents representing children who are not receiving Temporary Assistance for Needy Families. Information is also shared with state agencies managing child welfare or foster care programs, unemployment insurance programs, and with agents or attorneys responsible for establishing or enforcing child custody or visitation orders. Additionally, information may be shared with courts or government agencies dealing with cases of child abduction or unlawful taking or restraint of a child.

Specified data is also shared with federal agencies like the Department of the Treasury, Department of State, Department of Education, Department of Housing and Urban Development, and the Social Security Administration for purposes outlined in federal law, such as processing benefits or recovering unpaid debts.

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

The secondary use of PII from the NDNH is for research after the removal of personal identifiers (see 42 U.S.C. 653(j)(5)).
Specified analyses are conducted, as well as research for purposes found by the Secretary to be likely to contribute to achieving the purposes of Title IV, Part A, of the Social Security Act (42 U.S.C.

§§ 601 through 619), or Title IV, Part D, of the Social Security Act (42 U.S.C. §§ 651 through 669b).

OCSS receives numerous requests for information maintained in the NDNH for comparisons with other information for various purposes. Section 453 of the Social Security Act (42 U.S.C. § 653) governs the NDNH and specifies the entities authorized to
request and receive NDNH information and the purposes for which the information may be used.

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

Section 453 of the Social Security Act provides the legal basis for how the system can maintain, use, and disclose the information it collects. Section 453(l) and (m) and section 454(26) govern restrictions on disclosure and use of the information, and the confidentiality and safeguards around disclosing this information to ensure it is only shared with authorized entities. [Social Security Act (42 U.S.C. §§ 653(l), (m), and 654(26))].

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.

OCSS National Directory of New Hires, 09-80- 0381, April 11, 2024 (89 FR 2562)

Identify the sources of PII in the system.

Government Sources

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

Non-Government Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

The OMB (Office of Management and Budget) Control Number for this information collection is 0970-0166. This number indicates that OMB has approved the collection of this information for a period of three years. The current approval is valid until July 31, 2025.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

There are agreements in place that authorize the sharing or disclosure of information. These include Computer Matching Agreements (CMA), which allow data comparison between agencies to verify information, and Memorandums of Understanding (MOU), which document the terms and conditions for sharing data and information resources in a secure manner, define the purpose of the interconnection, identify relative authorities, and specify the responsibilities of the participating organizations.

Some agencies also require Information Sharing Agreements (ISA) to establish an agreement regarding the development, management, operation, and security of the connection between the agencies.

NDNH disclosures are mandated, authorized, and detailed in section 453(j) of the Social Security Act. [(42 U.S.C. § 653(j))].

Describe the procedures for accounting for disclosures.

OCSS establishes an agreement, either an MOU or CMA, with each agency that receives NDNH information. These agreements specify the purpose of sharing the information, the legal authority that allows it to be shared, and the expected results. The agreements also include a description of the records and details on how the records will be used, how long they will be kept, how they will be disposed of, terms for agency reimbursement, security requirements, and performance reporting requirements.

A security addendum is attached to every data sharing agreement. Before any agency receives NDNH information, an authorized
agent from that agency must sign the security addendum. This security addendum outlines the necessary security measures and safeguards the agency must have in place before receiving NDNH information.

OCSS tracks the disclosure of information by recording the signature date of the MOU or CMA and the specific purpose of the data match, ensuring accountability for each disclosure. All of these procedures for sharing and tracking the information are required by federal law and guidance. [Privacy Act of 1974 (5 U.S.C. § 552a), Federal Information Security Management Act of 2014, NIST Special Publication (SP) 800-47, Rev 1, NIST SP 800-53, Rev 5, OMB Circular A-130, and OMB Memorandum
M-17-12].

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Notification Requirements: Notification to individuals is not required because the collection of this information is mandated by federal statutes.

Source of Information: The NDNH primarily contains information provided on Internal Revenue Service (IRS) Form W-4. This information is not collected directly from individuals but is submitted to OCSS by the State Directories of New Hires (SDNH) and employers. The IRS W-4 form informs individuals through the form’s Privacy Act and Paperwork Reduction Act Notice that their information will be shared with the NDNH.

Data Retention and Modification: Information maintained in the NDNH is deleted 24 months after it is entered. Intentional modifications to the data are rare and occur only when information is used for research purposes, during which PII is de- identified and replaced with pseudo elements to prevent re- identification. [Social Security Act, 42 U.S.C. §§ 653(i)(2)(A), and (j)(5)].

Data Access and Security: Role-Based Access Control is in place to ensure that PII is only available to individuals who need it to complete their tasks. Non-repudiation measures are in place to ensure accountability, tracking the actions of those handling PII.

Employer Reporting Obligations: Employers are required to submit a report to the SDNH of the state where a newly hired employee works. This report includes the employee's name, address, SSN, the date the employee first performed services for pay, as well as the employer's name, address, and identification number assigned under Section 6109 of the Internal Revenue Code of 1986. [Social Security Act, 42 U.S.C. § 653A(b)(1)].
Definition of "Employer": For New Hire reporting purposes, the definition of an "employer" is the same as for federal income tax purposes, including governmental entities and labor organizations, as defined by section 3401(d) of the Internal Revenue Code of 1986 [Social Security Act, 42 U.S.C. § 653A(a)(2)(B)]. At a minimum, in any case where an employer is required to have an employee complete a W-4 form, the employer must meet the New Hire reporting requirements.
Reporting Forms: Employers can report new hires to the SDNH either by submitting a copy of the W-4 form or an equivalent form developed by the employer. Some states have developed an alternate form for reporting, but its use is optional. [Social Security Act, 42 U.S.C. § 653A(c)].
Legislative Mandate for PII: The PII contained in the NDNH system (OMB Information Collection No. 0970-0166) comes from mandatory legislative requirements. Employers must submit new hire information collected on the W-4 form from new employees. Employers then submit new hire and quarterly wage information to the SDNH, which subsequently forwards it to the NDNH. Employers and federal agencies are further required to submit new hire, quarterly wage, and UI information as required by federal law. [Social Security Act, 42 U.S.C. §§ 653 and 653A].

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

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.

Legal and/or statutory provisions require the collection and use of PII in the NDNH, so there is no method for individuals to opt-out of this information collection. The requirements for collecting this information are outlined in sections 453 and 453A of the Social Security Act. [42 U.S.C. §§ 653 and 653A].

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

Individuals are not notified directly when major changes occur to the NDNH, such as changes in data usage or disclosure. This is because the collection and use of PII in the NDNH are mandated by federal law, as outlined in section 453A of the Social Security Act. [42 U.S.C. § 653A]. Due to this statutory requirement, obtaining consent or providing direct notifications to individuals is not feasible. However, when major changes to the system occur—such as updates in how data is disclosed or used—these changes are made publicly available through the publication of a System of Record Notice (SORN) in the Federal Register. The SORN outlines any changes to data collection, storage, use, or disclosure and serves as a formal notice to the public about how their information is handled. This ensures transparency even though direct notification is not required by law.

For example, the most recent SORN for the NDNH, detailing a new data use policy, was published on April 11, 2024 (89 FR 2562), under the OCSS National Directory of New Hires SORN, 09-80-0381. Individuals can access this notice through the Federal Register to stay informed about any significant changes to the system.

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.

Information on notification, access to records, and contest procedures are published in the Federal

Register at 89 FR 25631. Record Access Procedures:
To request access to a record about you in this system of records, submit a written access request to the System Manager. The request must include your name, telephone number or email address, current address, signature, and sufficient particulars (such as date of birth or SSN) to enable the System Manager to distinguish between records on subject individuals with the same name. To verify your identity, your signature must be notarized, or your request must include your written certification that you are the individual who you claim to be and that you understand that the knowing and willful request for, or acquisition of, a record pertaining to an individual under false pretenses is a criminal offense subject to a fine of up to $5,000.
Contesting Record Procedures:
To request correction of a record about you in this system of records, submit a written amendment request to the System Manager. The request must contain the same information required for an access request and include verification of your identity in
the same manner required for an access request. In addition, the request must reasonably identify the record and specify the information contested, the corrective action sought, and the reasons for requesting the correction; it should include supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

Notification Procedures:
To find out if this system of records contains a record about you, submit a written notification request to the System Manager. The request must identify this system of records, contain the same information required for an access request, and include verification of your identity in the same manner required for an access request.

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 PII in the NDNH is not subject to periodic reviews within the system because the accuracy of the data is the responsibility of the state or federal agencies that submit it. Each agency is required to ensure the accuracy and relevance of the data before transmitting it to the NDNH.

Although the system does not conduct periodic reviews of the data itself, OCSS ensures that confidentiality, integrity, and availability of the files are maintained by meeting strict security requirements. OCSS contractors implement security measures in accordance with the Federal Information Processing Standards (FIPS) 199, which classifies the system as “moderate” risk. This classification means that the system follows government standards for protecting data and ensuring its availability and integrity.
Additionally, the system must comply with all necessary cybersecurity requirements to obtain and maintain its Authorization to Operate (ATO). This authorization is granted only when the system demonstrates it meets federal standards for security and reliability.

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.

All system users who access PII are specifically authorized based on their roles and responsibilities within the system. For example, administrators, developers, and contractors are only granted access to the information they need to perform their job duties.

State users are authorized by their respective state agencies to access PII as required for fulfilling child support services or other relevant functions.

Proper administrative procedures, such as background checks, and security measures, such as Role Based Access Controls (RBAC), are in place to ensure that the individuals with access to PII are vetted and have followed all required policies and procedures and have taken all required training.

Role Determination:
Identify the user's role (e.g., administrator, developer, contractor, or state user).
Determine the specific responsibilities associated with that role and the level of access to PII that is required for the user to fulfill their duties.
Authorization by State or Agency:
• For state users, the state agency must authorize the individual’s access to the system.
• For federal employees or contractors, the respective department or agency must grant authorization based on the user’s role and responsibilities.
Background Check:
• Conduct a background check on all individuals who require access to PII.
• Verify that the individual has passed the background check and meets the necessary qualifications before proceeding to the next step.
RBAC Implementation:
• Implement RBAC for each user, ensuring they can only access the data necessary for their specific job duties.
• Configure system permissions to limit access based on the user’s role and ensure they cannot access information outside their scope of responsibility.
Completion of Required Policies and Procedures:
• Ensure that the user has reviewed and agreed to comply with all required policies and procedures related to data access and PII handling.
• Confirm that the user is aware of the rules governing the use of PII, including any specific policies implemented by the agency or system administrator.
Mandatory Training:
• Require the user to complete mandatory training on data privacy, legal requirements, and system security protocols before being granted access to PII.
• Verify that the user has completed the training and understands the security requirements involved in handling sensitive information.
Final Authorization and Access Grant:
• Once all previous steps are completed (role determination, background check, RBAC configuration, policy agreement, and training), the user can be granted access to the system containing PII.
• Once all previous steps are completed (role determination, background check, RBAC configuration, policy agreement, and training), the user can be granted access to the system containing 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.

The principle of Least Privilege is maintained throughout the system, meaning that only those who need access to PII to perform or accomplish specified tasks are granted access to PII.

Least Privilege: The system enforces the principle of Least Privilege, ensuring that individuals with access to personally identifiable information (PII) are only granted access to the minimum amount of information necessary to perform their specific job functions.

RBAC: To enforce the principle of Least Privilege, the system employs RBAC, which restricts user access to PII based on their job roles. Each user is assigned a role that corresponds with their responsibilities, and their access is limited to the data required to complete their tasks. For example, administrators may have broader access to manage the system, while developers or contractors only have access to PII when it is necessary for maintenance or support.

Audit Logs: Additionally, audit logs are maintained to track who accesses PII and when, allowing system administrators to monitor and review access to ensure compliance with the principle of Least Privilege.
Access Reviews: Regular access reviews are conducted to confirm that users still require the level of access they have been granted and to adjust permissions as needed.

This combination of RBAC, monitoring through audit logs, and regular access reviews ensures that users only access the
minimum amount of PII necessary to perform their job functions.

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.

New hire orientation, Computer Awareness and Record Management, and annual security awareness training is required for all users with access to the system. Training is provided by HHS, the Administration for Children and Families (ACF), and OCSS.

All personnel with access to the system, including system owners, managers, operators, contractors, and program managers, are required to complete a series of training programs to ensure they are aware of their responsibilities for protecting the information collected and maintained in the system.

New Hire Orientation: This training is mandatory for all new employees and contractors. It introduces them to the security policies and procedures they must follow when handling PII in the system.

Computer Awareness and Record Management Training: This training provides personnel with knowledge of cybersecurity best practices, data management, and the proper handling of sensitive records. It covers topics such as data classification, access control, and secure data disposal.

Annual Security Awareness Training: This training is required for all system users on an annual basis to reinforce key security principles, including protecting sensitive data, recognizing phishing attacks, and reporting security incidents.

All training is provided by HHS, ACF, and OCSS. These training programs ensure that all personnel remain aware of their legal and ethical obligations to protect the information within the system and comply with relevant security policies.

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

Currently, no training beyond general security and privacy awareness is provided to system users. The existing training program—consisting of annual security awareness training, role- based training, and refresher courses—fully equips personnel to handle PII in accordance with applicable laws and regulations.

This comprehensive training covers key areas, including understanding legal requirements (such as IRS regulations and federal statutes), role-specific data handling practices, and cybersecurity awareness. It is designed to ensure all users, regardless of role, are knowledgeable and capable of protecting sensitive information.

This robust general training program is sufficient to meet the security and privacy needs of the system.

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 process is described in National Archives and Records Administration (NARA) Job # N1-292-10-002, ACF OCSS NDNH Electronic Records Schedule:

The process for retaining and destroying PII in the NDNF system follows both statutory requirements and NARA guidelines.

Retention Process: Records are deleted from the NDNH database 24 months after the date of entry. [Section 453(i)(2) of the Social Security Act. [42 U.S.C. § 653(i)(2)].
For quarterly wage and unemployment insurance (UI) information, OCSS loses access to this data after 12 months, unless a match occurs from information comparison. [Section 453(i)(2) of the Social Security Act. [42 U.S.C. § 653(i)(2)].

Destruction Process: After the 24-month cutoff, records are permanently deleted in accordance with the statutory timeline [42
U.S.C. § 653(i)(2)(A)]. Records are kept temporarily, cut off quarterly, and then deleted 24 months after cutoff.

Exceptions for Research: Under certain conditions, OCSS may retain samples of data from the NDNH for research purposes that align with the objectives of Part A or Part D of Title IV of the Social Security Act [42 U.S.C. §§ 601 through 619 and 42 U.S.C.
§§ 651 through 669b]. To ensure privacy, these samples do not contain personal identifiers. The retention period for these samples is limited to the time necessary to complete the research. [Social Security Act, 42 U.S.C. §§ 653(i)(2)(C) and 653(j)(5)].

Disposition: Records are kept temporarily, cut off quarterly, and deleted 24 months after cutoff, pursuant to section 453(i)(2) of the Social Security Act. [42 U.S.C. § 653(i)(2)].

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

The NDNH system employs a moderate security classification under FIPS 199, ensuring appropriate protection for sensitive PII through a combination of administrative, technical, and physical controls.

Administrative Controls: Access to PII is strictly regulated, with users required to complete security awareness training upon hiring and annually. They must also sign the HHS and OCSS Rules of Behavior and a non-disclosure oath. Access is managed under the principle of least privilege, and compliance is verified through regular audits.

Technical Controls: Strong authentication measures such as passwords, tokens, and PIV cards are required for access. Encryption protects data at rest and in transit, and Role-Based Access Controls (RBAC) ensure that only authorized users can access sensitive information. Firewalls, intrusion detection systems, Virtual Private Networks (VPNs), and continuous vulnerability monitoring help safeguard against external threats.

Physical Controls: System facilities are highly secured, with access restricted to authorized personnel using government-issued IDs. Visitors must be vetted and escorted, while cameras and security audits help maintain a strong security posture.

Additionally, OCSS reinforces security awareness through mandatory training and compliance measures, ensuring personnel adhere to established security protocols and protect sensitive data.