US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/21/2016

OPDIV:

ACF

Name:

National Directory of New Hires

PIA Unique Identifier:

P-1179540-207940

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.

N/A

Describe the purpose of the system.

The National Directory of New Hires (NDNH) is a national repository of employment information. It accepts New Hire and Quarterly Wage (QW) information from States, US territories (Guam, Puerto Rico and the Virgin Islands), and Federal agencies. From States and two US territories (Puerto Rico and the Virgin Islands) NDNH also receives Unemployment Insurance (UI) benefit information.

The NDNH interacts with other systems in the Federal Parent Locator Service (FPLS). Its primary purpose is to assist state child support agencies locate noncustodial parents, putative fathers, and custodial parents to establish paternity and child support obligations, as well as to enforce and modify orders for child support, custody, and visitation.

The Multi-State Employer Registry (MSER) is a sub-system of the NDNH. Social Security Act § 453 (i)(4), 42 U.S.C. § 653(i)(4) requires the Secretary of Health and Human Services to maintain within the NDNH a list of multistate employers that are exercising the option to report to one State and the State to which the employer is reporting. OCSE sends that list to each State Directory of New Hires on a monthly basis. The MSER is covered under the Federal Parent Locator Services (FPLS) iPortal PIA.

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

The personally identifiable information collected is as follows:

1. Records pertaining to newly hired employees furnished by a State Directory of New Hires pursuant to Social Security Act § 453A(g)(2)(A), 42 U.S.C. § 653a(g)(2)(A). Records in the system are the first and last name, mailing address, date of hire, and Social Security number (SSN) of the employee and the name, address, and federal identification number (FEIN) of the employer of such employee .
2. Records pertaining to newly hired employees furnished by a Federal department, agency or instrumentality pursuant to Social Security Act § 453A(b)(1)(C), 42 U.S.C. § 653a(b)(1)(C). Records in the system are the first and last name, mailing address, date of hire, and SSN of the employee and the name, address and FEIN.
3. Records furnished by a State Workforce Agency pertaining to wages and unemployment compensation paid to individuals pursuant to Social Security Act § 453A(g)(2)(B), 42 U.S.C. § 653a (g)(2)(B). UI data elements collected are: claimant SSN, claimant name, claimant address, claimant benefit amount, and reporting period
4. Records furnished by a Federal department, agency, or instrumentality pertaining to wages paid to individuals pursuant to Social Security Act § 453(n), 42 U.S.C. § 653(n). System users access the data after signing on to production system via user ID and password. Data is secured to authorized users via Resource Access Control Facility (RACF).
5. The NDNH collects new hire information from Guam, Puerto Rico and the Virgin Islands. The information includes the employee first and last name, mailing address, SSN, date of hire, and date of birth (optional). In addition, the employers name, address, and FEIN associated with each new employee reported. Note that "New Hire" is the type of information not necessarily new information. Date of Birth (DOB) is an optional field in the NDNH system. Military status information is collected by another OCSE system which is covered under a different PIA.

The NDNH requires administrators and contractors to provide multi-factor authentication such as; user credentials such as a user name and password, a personal identity verification (PIV) card and/ other "something you know" questions.

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 State Directory of New Hires (SDNH). Federal agencies report directly to the NDNH. Employers are required to report: Employee name, Employee Social Security number, Employee mailing address, Employer name, Federal Employer Identification Number (FEIN), Employer address, and Date of hire. Note that "New Hire" is the type of information not necessarily new information.

The Quarterly Wage (QW) File contains quarterly wage information on individual employees from state workforce agency (SWA) and federal agency record. NDNH receives: Employee name (if collected by the state), Employee Social Security number, Employee wage amount, Reporting period (calendar quarter in which wages were paid), Employer name, FEIN, Employer address, Employer optional address.

The Unemployment Insurance (UI) File contains unemployment insurance 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 Social Security number, Claimant mailing address, Claimant benefit amount (gross amount before any deductions), Reporting period (calendar quarter in which the UI claim was filed).

The data is kept temporarily in accordance with a registered disposition with NARA Job # N1-292-10-002. Per Social Security Act § 453(i)(2), 42 U.S.C. § 653(i)(2), records are deleted from the database 24 months after date of entry into the NDNH.

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

Employer Federal Identification Number (FEIN)

User credentials (user id and password)

Income

Date of hire

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 the NDNH is to improve States' abilities to locate parents and collect child support. Additional purposes of the NDNH include assisting authorized Federal and State agencies in establishing or verifying eligibility of applicants for, or beneficiaries of, Federal or State benefit programs; recouping payments or delinquent debts under such benefit programs.

State Child Support Enforcement (CSE) Agencies provide valuable information such as: location information about noncustodial parents in child support cases; paternity results; and which states have primary court jurisdiction that enables them to establish, set, modify, or enforce child support obligations, and enforce child support orders.

Federal law authorizes that specified types of collected information may be shared with specified entities for specified purposes. In summary, the collected information is shared with the following entities: State Child Support Enforcement (CSE) agencies; a court with authority to issue a child support order; a resident parent, legal guardian, attorney, or agent of a child who is not receiving Temporary Assistance for Needy Families (TANF); a state agency administering specified child welfare or foster care programs; a state agency administering the Unemployment Compensation program; an agent or attorney of a state, with an agreement, who has the duty or authority under state law to enforce a child custody or visitation determination; a court having jurisdiction to make or enforce a child custody or visitation determination; and an agent or attorney of a state or the United States with responsibility for matters involving the unlawful taking or restraint of a child.

Specified information is also shared with the following Federal agencies for the authorized purposes specified in Federal law: Department of the Treasury; Department of State; Department of Education; Department of Housing and Urban Development; and the Social Security Administration.

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

The secondary use of PII from the NDNH is research. Specified analysis is conducted after the removal of personal identifiers, as well as for providing access to data for research purposes found by the Secretary to be likely to contribute to achieving the purposes of Social Security Act Title IV, Part A, 42 U.S.C. §§ 601 through 619, or Social Security Act Title IV, Part D, 42 U.S.C. §§ 651 through 669b. Personal identifiers are also removed prior to providing any data access.

OCSE receives numerous requests for information in the NDNH for comparisons of NDNH information with other information for various purposes. Title IV-D of the Social Security Act, which governs the NDNH and specifies the entities authorized to request NDNH information and the purposes for which the information may be used.

Describe the function of the SSN.

SSN is the Primary index key for information stored in NDNH.

Cite the legal authority to use the SSN.

Social Security Act § 452(a)(7) and (9), 42 USC § 652(a)(7) and (9)
Social Security Act § 453, 42 U.S.C. § 653, generally
Social Security Act § 459A, 42 U.S.C. § 659A
Social Security Act § 463, 42 U.S.C. § 663

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

Social Security Act § 453(l) and (m), 42 U.S.C. § 653(l) and (m)
Social Security Act § 454(26), 42 USC § 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.

09-80-0381 April 2, 2015 (80 FR 17906)

09-80-0381 1/5/2011

Identify the sources of PII in the system.

Government Sources

State/Local/Tribal

Other Federal Entities

Identify the OMB information collection approval number and expiration date

OMB NO: 0970-0166 Filed 2/29/2016

Is the PII shared with other organizations?

Yes

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

Other Federal Agencies

Provisions of the law, eligibility identification/verification

State or Local Agencies

Primarily for location and identification of child support obligators

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

There are agreements in place developed and executed accordingly for any approved disclosures. Computer Matching Agreements (CMAs) or Memorandum of Understanding (MOUs) are in place with all federal agencies where data is shared. Information Sharing Agreements (ISAs) are used where the partner agency requires.

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

Describe the procedures for accounting for disclosures.

OCSE enters into a Memorandum of Understanding (MOU)/Computer Matching Agreement (CMA) with each agency that receives NDNH information. The MOU/CMA describes the purpose, legal authority, justification, expected results of the match, description of the records, retention and disposition of information, reimbursement, and performance reporting requirements. Each agency is required to sign the security addendum, which is a component of the MOU/CMA. The security addendum provides a detailed description of the security requirements and safeguards that an agency must have in place before receiving NDNH information.

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 of individuals is not required as information is collected based on mandatory federal statutes. Information collected is never unintentionally destroyed; according to the Security Act § 453(i)(2), 42 U.S.C. § 653(i)(2) information is deleted 24 months after date of entry into the National Directory of New Hires (NDNH). Intentional modification only occurs when data is used for research purposes; PII is de-identified, and replaced with pseudo elements to prevent re-identification. Role-Based Access control is in place to ensure that PII is available only to those who need to know, and for the fulfillment of assigned tasks. Additionally non-repudiation measures are in place to ensure that those handling PII are accounted for and their actions are tracked.

Per Social Security Act § 453(i)(2), 42 U.S.C. § 653(i)(2)

1) Each employer shall furnish to the Directory of New Hires of the State in which a newly hired employee works, a report that contains the name, address, and social security number of the employee, the date services for remuneration were first performed by the employee,[186] and the name and address of, and identifying number assigned under section 6109 of the Internal Revenue Code of 1986[187] to, the employer.

2) Federal law states that an "employer" for New Hire reporting purposes is the same as for federal income tax purposes (as defined by Section 3401(d) of the Internal Revenue Code of 1986) and include any governmental entity or labor organization.

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.

3) Employers have the option to report new hires to their State Directory of New Hires either on a copy of the W-4 form or, by an equivalent form developed by the employer. Some states have developed an alternate form for reporting, but its use is optional.
4) Records are deleted from the database 24 months after date of entry into the NDNH.

Further clarification into understand why collection of PII is mandatory in this system: . The PII in the NDNH system (PRA number 0970-0166) pertains to the legislative requirement, mandatory for employers, to submit new hire information collected on the W-4 form, which is completed by individuals. Employers then submit new hire and quarterly wage information to their State Directory of New Hires which in turn is submitted to the NDNH. The new hire, quarterly wage and unemployment insurance information is legislatively mandated to be collected by employers and federal agencies, which is why we selected mandatory.

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 of and use of PII in the NDNH. There is no opt-out option since this collection is mandatory under Federal Statute - SEC. 453A [42 U.S.C 653a] of the Social security Act.

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

Consent is not required because the information collected is mandated by federal statute (SEC. 453A [42 U.S.C 653a] of the Social security Act.). Data use is published in the NDNH System of Records Notice (SORN) in the Federal Register.

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.

Notification is to be sent to the Office of Child Support Enforcement (OCSE). Additional information on notification procedures, including the who and how, is provided in the Federal Register (80 FR 17906). The information obtained inappropriately or being contested must be specified along with supporting justification to show how the record is inaccurate, incomplete, untimely, or irrelevant and the corrective action sought.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Federal law requires that OCSE implement safeguards to restrict access to NDNH information to authorized persons and restrict the use of the information to authorized purposes. Internal systems are continuously monitored to ensure system security and recipients of NDNH information must agree to comply with security safeguards, such as:
Operational safeguards that ensure NDNH information is secure from unauthorized persons and unauthorized uses at all times.

Technical safeguards that ensure NDNH information is stored and transmitted in a secure manner and that information is processed using methods that protect the confidentiality of the information. Only those with the need to know can access PII only for the specified tasks. NIST 800-53 requirements such as AC-6 Least Privilege principle is followed to ensure that only authorized users have access to the data they need to accomplish assigned tasks. Management safeguards that require written information technology security policies and procedures, notification to OCSE of any breach in access to the information and agreement to allow onsite monitoring or verification by OCSE to ensure compliance with security requirements.

FISMA, OMB requirements are adhered to ensure a robust security posture of PII data contained in NDNH.

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

Users:

After a successful login users have access to their own PII.

Administrators:

(Direct Contractors) Privileged users within the federal departments can access PII for administering (ie. income tax credit), verifying claims, or collecting debt owed to the federal government

Developers:

(Direct Contractors) Conduct enhancements and maintenance, Production Support: operations and technical support

Contractors:

Contractors work on behalf of state or federal government to ensure Child Support Enforcement, and to deliver on social security Act requirements. Some developers are contractors supporting the security of NDNH system environment.

Others:

US territories will have access as Child Support Enforcement Agencies for child support enforcement purposes.

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

All users are specifically authorized by their roles. State users are authorized by the state agency. Proper administrative procedures such as back ground 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, procedures and required training.

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 the only ones granted access to PII.

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. Training is provided by HHS, ACF and by Office of Child Support Enforcement (OCSE).

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

Annual training includes IRS regulations, Federal statutes, HHS and ACF regulations, and refresher training. Role based training is also required.

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.

There is a registered Disposition with NARA Job # N1-292-10-002. Per Social Security Act § 453(i)(2), 42 U.S.C. § 653(i)(2), records are deleted from the database 24 months after date of entry into the NDNH.

Additionally, in accordance with Social Security Act § 453(i)(2)(B), 42 U.S.C. § 653(i)(2)(B), OCSE shall not have access for child support enforcement purposes to quarterly wage and unemployment insurance information in the NDNH, if 12 months have elapsed since the information is provided by a State Directory of New Hires pursuant to Social Security Act § 453A(g)(2)(B), 42 U.S.C. § 653a(g)(2)(B) and there has not been a match resulting from the use of such information in any information comparison. Notwithstanding these retention and disposal requirements, OCSE may retain such samples of data entered into the NDNH as OCSE may find necessary to assist in carrying out its responsibility to provide access to data in the NDNH for research purposes found by OCSE to be likely to contribute to achieving the purposes of Part A or Part D of Title IV of the Act, 42 U.S.C. §§ 601 through 619 and 42 U.S.C. §§ 651 through 669b, but without personal identifiers, pursuant to Social Security Act §§ 453(i)(2)(C) and 453(j)(5), 42 U.S.C. §§ 653(i)(2)(C) and 653(j)(5). Samples are retained only so long as necessary to complete such research.

Disposition: Records are kept temporarily; records are cut off quarterly. Records are deleted 24 months after cutoff, per Social Security Act § 453(i)(2), 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 information is secured in accordance with a system classified as "moderate" according to FIPS 199. The security controls are specified in an up-to-date system security plan (SSP). This SSP restricts access and disclosure to persons as authorized in the statute, provides administrative, physical, and technical system controls.

Technical controls include access controls with strong passwords, tokens, PIV cards, encryption of data in transmission and at rest, RBAC, separation of duties, auditing tools and logs, monitoring and scanning for vulnerabilities. Intrusion detection systems, firewalls, Virtual Private Networks, and demilitarized zones DMZs) are implemented.

Physical controls include; restricted access to facilities, secured system locations, and continued audits to ensure robust security posture. Employees have to use government issued IDs, and visitors are vetted and escorted at all times. Cameras are strategically located at entry and exit points. The system requires monitored access and OCSE promotes security training. All personnel with access to the system are required to sign the HHS and OCSE Rules of Behavior and sign a non-disclosure oath upon completing security awareness training as a new hire and then annually.