Privacy Impact Assessment
for the

Enterprise Human Resources Integration (EHRI)

Data Warehouse (DW)

January 29, 2016

Contact Point

Victor A. Karcher Jr.
EHRI Director

Reviewing Official

Cord E. Chase
Chief Security Officer
U.S. Office of Personnel Management

SECTION 1: PIA SUMMARY INFORMATION

a. Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the program office who own(s) the system;

- The business purpose of the program, IT system, or technology and how it relates to the program office and Agency mission;

- A general description of the information in the IT system;

- A description of a typical transaction conducted on the IT system;

- Any information sharing conducted by the program or IT system;

- A general description of the modules and subsystems, where relevant, and their functions; and

- A citation to the legal authority to operate the program or IT system.

The EHRI Data Warehouse (DW) serves a comprehensive electronic personnel record-keeping and analysis system that supports Human Resource (HR) management reporting across the Federal government. This system spans the career of 2.2 million Executive Branch civilian Federal employees from hiring to retiring and provides agency HR professionals with access to Federal employee HR, Payroll, Training, and Retirement data.

The EHRI DW provides agency HR Specialist and managers with an array of workforce analytical and planning capabilities for all data contained within the DW. Through this common repository of HR, Payroll, Training, and Retirement data, DW users are able to query workforce data from a variety of perspectives for planning and analytical purposes to determine statistical counts, averages, trends, promotions, reassignments, and other significant personnel actions. Together, the tools available within the EHRI DW will enable a new level of strategic planning and reporting not previously available. The EHRI DW receives HR, Payroll, Training, and Retirement data from agencies and Shared Service Centers (SSCs), Human Resource Information Systems (HRIS), Payroll Systems, Learning Management Systems (LMSs), and Retirement Data Providers in accordance with the Guide to Human Resources Reporting (GHRR) and Guide to Retirement Data Reporting (GRDR). .

The EHRI Data Warehouse system consists of the following subsystems or minor applications;
EHRI Data Warehouse - Oracle repository consisting of HR, Payroll, Training, and Retirement Data

Statistical Data Mart (SDM) – Oracle repository consisting of cleansed HR data for official reporting purposes.

Central Employee Record (CER) - A web-based application for performing individual employment history searches and lookups.

Business Intelligence (BI) - Business Object applications providing users with ad-hoc query and reporting capabilities, as well as dash boarding of statistical measures.

Data Quality Reporting System (DQRS) - Provides data providers with reporting regards errors from data submission files.

Retirement Data Viewer (RDV) – An application that allows Retirement adjudicators the ability view Individual Retirement Records (IRR) and data received from Retirement Data Providers for comparison when adjudicating retirement claims

One Data - Integrated metadata repository.

Data Standards - Definition of data elements in EHRI and on personnel actions.

b. Why is this PIA being created or updated? Choose one:

☐ **New OPM Information System** ☐ **New Electronic Collection**

☒ **Existing OPM Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified OPM Information System**

c. Does the OPM information system or electronic collection have a Privacy Act System of Records Notice (SORN)?

Enter the SORN number only in the above text box. If there is a question regarding the existence of a SORN or if a SORN needs to be created or updated, contact your Privacy Official with any questions regarding SORN issues.

NOTE: A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is <u>retrieved</u> by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes**   **Enter Privacy Act SORN Number/Name** | OPM/GOVT-1 |

or

☐ **No**   **Date of submission for approval to OPM Privacy Office** | |
Consult the Privacy Office for this date.

d. Summary of OPM information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

    (1)   Describe the purpose of this OPM information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

- Describe purpose - State why this system contains an individual's PII and how it is used and protected. Write a brief detailed statement that a layman can understand.

- Identify and list all PII that is collected and stored in the system. This could include, but is not limited to: name, date of birth, mailing address, telephone number, social security number, email address, zip code, facsimile number, mother's maiden name, medical record number, bank account number, health plan beneficiary number, any other account numbers, certificate/license number, vehicle identifier including license plate, marriage record, civil or criminal history information, device identifiers and serial numbers, uniform resource locators (URLs), education record, Internet protocol addresses, biometric identifier, photographic facial image, or any other unique identifying number or characteristic.

- If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

- If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

The EHRI DW is a repository of HR, Payroll, Training, and Retirement data, which by its very nature is contains PII. The Guide to Human Resource Reporting (GHRR) and the Guide to Retirement Data Reporting (GRDR) contains the data elements captured in the DW repository.

      (2)   Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

- Collectively describe the potential risks involved with the collection and discuss the mitigation for each risk identified.

Privacy risks to information in the EHRI DW include the inadvertent or unintentional disclosure, alteration, or deletion of data. These risks are mitigated through the implementation and testing of systems security controls.

e. Retention of Information. Does this information system or electronic collection retain information? Contact the OPM Records Management Office for this information.

- Identify and list all information collected that is retained by the system.

- In some cases OPM may choose to retain files in active status and archive them after a certain period of time. State active file retention periods as well as archived records, in number of years, as well as the General Records Schedule. The OPM records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. See the OPM Records Management Handbook located at http://theo.opm.gov/References/IT/policies.asp

- An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The OPM records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the OPM records officer will notify the system owner. See the OPM Records Management Handbook located at http://theo.opm.gov/References/IT/policies.asp for additional information on retention schedules.

☒ **Yes**

Information Retained

All data elements as outlined in the GHRR and the GRDR.

Time period for retained information

> 5 U.S. Code § 8345, i, 1, (i)(1) No payment shall be made from the Fund unless an application for benefits based on the service of an employee or Member is received in the Office of Personnel Management before the one hundred and fifteenth anniversary of his birth.

Retention Schedule Name

> 36 CFR, General Records Schedule 1, and
> General Records Schedule 20, 5 U.S.C §
> 8345, i, 1, (i)(1)

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or OPM requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this OPM information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

      (a) Whenever possible, cite the specific provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

      (b) If a specific statute and/or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

      (c) OPM Program Offices can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive or instruction implementing the statute within the OPM Program Office should be identified. (e.g., Privacy Act of 1974)

> The e-Gov Act of 2002, Government Paperwork Elimination Act of 1998, 5 CFR Chapter 1 parts 110 and 293, and the OPM Government-Wide System of Record Notice (SORN) (OPM/GOVT-1), General Personnel Records and OPM/Central-1, Civil Service Retirement and Insurance Records under the Privacy Act of 1974 as amended

g. Information Retrieval. How is the information retrieved? (By name, SSN, etc)

The ability to retrieve information is based on the user role within the EHRI DW. User roles determine what data will be visible to a particular user. Types of users are: Agency Operating Personnel, Agency Data Analyst, Agency Data Administrator,, Government Wide Data Analyst, Government Wide Super User, and EHRI User Administrator/Tool Access Management. The Government Wide
Super User can access all data within EHRI DW.

The Retirement Data Viewer employs role-based access control. User roles are assigned during user administration in EHRI's DW LDAP. The Retirement Data Viewer has the following user roles;   Retirement Data OPM Standard User, Retirement Data Agency Standard User; Retirement Data GRDR Technical Compliance User, Retirement Data GRDR Provider Role, Retirement Data Imaged Document Advanced User, and Retirement Data Application Administrator.

h. With whom will the PII be shared through data exchange, both within OPM and outside OPM (e.g., other Federal Agencies)? Indicate all that apply.

☒ **Within OPM. Specify**

Planning & Policy Analysis (PPA): PPA uses all of the applications within the EHRI DW. PPA using DW applications for planning and analysis support for the OPM Director and OPM with various reports as well as to respond to other government oversight entities such as the General Accounting Office (GAO). A particular area of responsibility is the analysis of policy options, legislative changes and trends that affect OPM's management of health and retirement benefits for Federal employees. To assure benefits provide maximum value and are secure, the office will conduct actuarial analysis as well as statistical tests using data sets contained within the EHRI DW.

Employee Services (ES): ES also uses all of the applications within the EHRI DW. ES provides policy direction and leadership in designing, developing, and promulgating government-wide human resources system and programs for recruitment, pay, leave, performance management and recognition, employee development, work/life/wellness programs and labor and employee relations. ES also provides technical support to agencies regarding the full range of human resources management policies and practices to include veteran's employment as well as the evaluation of their human resource programs. ES manages the operation of OPM's internal human resources program.

Merit System Audit & Compliance (MSAC): MSAC ensures through rigorous oversight that Federal agency HR programs are effective and meet merit system principles and related civil service requirements. Within the scope of their oversight, MSAC conducts HR evaluation of small agencies, examining a broad range of HR programs, including staffing and competitive hiring, performance management, and leadership and succession planning.

☒ **Other Federal Agencies. Specify** (agencies, not systems)

EHRI partners with all Executive Branch agencies to provide access to the EHRI DW. These Executive Branch agencies use personnel employee data and analytical tools in workforce planning and forecasting.

☐ State and Local Agencies. **Specify** (agencies, not systems)

☐ Contractor **(enter name and describe the language in the contract that safeguards PII.) Specify**

☐ Other (e.g., commercial providers, colleges). **Specify**

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes**   ☒ **No**

(1) If "Yes," describe the method by which individuals can object to the collection of PII. Include consequences, if any, if an individual objects.

(2) If "No," state the reason why individuals cannot object.

> Collection of PII is inherent in the HR processing of payroll and benefits for all Federal Employees.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes**   ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent. Include consequences, if any, if an individual withholds their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

> The EHRI DW does not directly collect information from individual. The EHRI DW is a repository of HR, Payroll, Training, and Retirement data, which is transmitted to the EHRI DW by providers or the employee's agency. Notice of how the information is used and shared is through routine uses under the OPM/GOVT 1 SCORN.

- Refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

- If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

- Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

- The issue of notice, particularly notice found in a SORN, involves the advice of counsel. Consult your assigned counsel on issues concerning the sufficiency of notice to the public on an information collection.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply. When collecting information from an individual, either in a paper or electronic collection, individuals have a right to understand the authority, purpose, routine uses that apply and the effects on the individual.

☐ **Privacy Act Statement**

☐ **Privacy Advisory**

☒ **Other**

☒ **None**

> Describe each applicable format.

> The EHRI DW is a repository of HR, Payroll, Training, and Retirement data, which is provided by the HR, Payroll, Training, and Retirement data providers via the employee's agency.
> Therefore, requests to provide information would be at the
> agency level and typically from the agency's HR department.

Privacy Act Statement - Give a PAS orally or in writing to the subject of the record when you are collecting information from them that will go in a system of records.

Privacy Advisory – Similar to a PAS, but is not covered by the Privacy Act. Information is being collected about an individual, but will not go into a formal system of records.

SECTION 2: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 2.a.(1) through 2.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

    (1) What PII will be collected? Indicate all individual PII or PII groupings that apply in the table below.

Non-Sensitive PII		
☒Name	☒Other Names Used	☒Marital Status
☒Work Cell Telephone Number	☒Work Telephone Number	☒Work Email Address
☒Emergency Contact	☒Salary	
Sensitive PII		
☒Social Security Number (SSN)	☒Truncated SSN	☒Driver's License
☒Personal Cell Telephone Number	☒Home Telephone Number	☒Other ID Number
☒Citizenship	☒Legal Status	☒Gender
☒Race/Ethnicity	☒Birth Date	☒Place of Birth
☒Mother's Maiden Name	☒Mother's Middle Name	☐Security Clearance
☒Personal Email Address	☒Mailing/Home Address	☒Spouse Information
☒Financial Information	☒Medical Information	☐Biometrics
☒Law Enforcement Information	☒Employment Information	☐Disability Information
☒Child Information	☒Education Information	☐Military Records
		☒Other

If "Other," specify or explain any PII grouping selected.

> The Guide to Human Resource Reporting (GHRR) and the Guide to Retirement Data Reporting (GRDR) contains the data elements captured in the DW repository.

(2) What is the source for the PII collected (e.g., individual, existing OPM information systems, other Federal information systems or databases, commercial systems)?

Describe.

> As mentioned, DW is a repository of HR, Payroll, Training, and Retirement data. The data sources are Federal HR providers, Payroll providers, Training providers, and Retirement Data providers.

How will the information be collected? Indicate all that apply.

☐ Paper Format   ☐ Face-to-Face Contact

☐ Telephone Interview   ☐ Fax

☐ Email   ☐ Web Site

☒ Information Sharing from System to System

☐ Other (Describe)

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Describe

> The EHRI DW is one of two systems that accomplish the mission of the EHRI program. Under the direction of the Office of Management and Budget (OMB), EHRI was established as one of five OPM-led e-Government initiatives designed to leverage the benefits of information technology as required by the e-Government Act of 2002. The overall goal of EHRI is to streamline and automate the exchange of Federal HR, Payroll, Training, and Retirement data government wide. The DW achieves this goal by providing a data repository of HR, Payroll, Training, and Retirement data.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Describe

> The intended use is to provide Executive Branch agencies and their HR specialists, statisticians, and analysts' access to a comprehensive Federal employee data for their agency through on-demand customer reports, ad-hoc reporting, and analytical reporting for Federal agencies

b. Does this OPM information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

☐ **Yes**

☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in the OPM information system or electronic collection? Indicate all that apply.

☒ **Users**   ☐ **Developers**   ☐ **System Administrators**   ☐ **Contractors**

☐ **Other** (Describe)

d. How will the PII be secured?

    (1) Physical Controls. Indicate all that apply.

☒ Security Guards
Identification Badges

☒ Cipher Locks

☒ Combination Locks
Closed Circuit Television

☐ Key Cards

☐ Safes

☐ Other   (Describe)

    (2) Technical Controls. Indicate all that apply.

☒ User Identification   ☐ Biometrics

☒ Password   ☒ Firewall

☒ Intrusion Detection System (IDS)   ☒ Virtual Private Network (VPN)

☒ Encryption   ☒ Public Key Infrastructure Certificates

☒ External Certificate Authority (CA) Certificate

☒ Other   (Describe)

IP Allow List, encryption of data in transit from providers

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits

☒ Regular Monitoring of Users' Security Practices

☒ Methods to Ensure Only Authorized Personnel Access to PII

☒ Encryption of Backups Containing Sensitive Data

☒ Backups Secured Off-site

☒ Security and Privacy Awareness Training

☒ Other (Describe)

Users must accept and adhere to the EHRI Rules of Behavior.

e. Does this OPM information system require an authorization and assessment under the OPM Authorization and Assessment Process?

☒ **Yes.** Indicate the certification and accreditation status:

ATO in review.

☐ Authorization to Operate (ATO) Date Granted:

☐ Denial of Authorization to Operate (DATO) Date Granted:

☐ Limited Authority To Operate (LATO) Date Granted:

☐ **No**, this OPM Information system does not require an authorization and assessment.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Describe.

The HR, Payroll, Training, and retirement providers send data to the EHRI DW using Connect:Direct, a FIPS 140-2 Compliant data transmission. Additionally, the EHRI DW works in accordance with Federal Information Processing Standards Publication (FIPS)199, Federal Information Security Management Act of 2002 (FISMA), NIST 800-37 and 800-53 rev4, Public Law 107-247, 44 U.S.C 3531-3536, and the Office of Management and Budget's (OMB)Circular A-130, Appendix III, Security of Federal Automated Information Systems.

g. For existing OPM information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Describe:

Risks identified in security controls testing during the A&A process and ongoing continuous monitoring are captured in eOPF Plan of Action and Milestones (POAMs). Mitigation strategies are noted and monitored until items are closed.

h. For new OPM information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe.

The EHRI DW is not a new OPM information system. Risks identified in security controls testing during the A&A process and ongoing continuous monitoring are captured in eOPF Plan of Action and Milestones (POAMs). Mitigation strategies are noted and monitored until items are closed.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the OPM Privacy Officer prior to being signed by the system owner, CISO or CIO.

System Owner

Signature: _V.A. Karch_

Digitally signed by VICTOR KARCHER
DN: c=us, o=U.S. Government, ou=Office of Personnel Management,
cn=VICTOR KARCHER, 0.9.2342.19200300.100.1.1=24001000033590
Date: 2016.01.29 14:38:47 -05'00'

Name: Victor A. Karcher, Jr.

Organization: CIO/FDS/Data Warehouse

Email Address: victor.karcher@opm.gov

Date of Review: 1/29/2016

Chief Information Security Officer

Signature: _[signature]_

Name: Cord Chase

Organization: OCIO

Email Address: Cord.Chase@opm.gov

Date of Review: 1/29/16

Chief Privacy Officer

Signature: _[signature]_

Name: Donna K. Seymour

Organization: CIO

Email Address: donna.seymour@opm.gov

Date of Review: 1/29/2016

For Official Use Only