US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/28/2016

OPDIV:

OS

Name:

Business Intelligence Information System

PIA Unique Identifier:
P-9037630-203854

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.
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.
None

Describe the purpose of the system.
The Business Intelligence Information System (BIIS) is a consolidated enterprise reporting and analytics system that collects, tracks, routes, maintains, and reports personnel, pay, attendance/leave, and other information relating to all HHS employees. BIIS is used by HHS staff to access the following systems: Enterprise Human Resources and Personnel System (EHRP), Time and Attendance (ITAS), Recruitment Enterprise Workflow Information Tracking System (EWITS), Defense Finance and Accounting Services, (DFAS), Learning Management System (LMS).

Also, BIIS is used to access the following types of information: Human Resources (HR), Budget, Workmen's Compensation, Payroll, Time and Attendance, and Equal Employment Opportunity (EEO) Information.

Information from the source systems is loaded into BIIS via recurring automated loads of datafiles sent to BIIS from the various source systems.

BIIS users such as HHS employees from all Operating Divisions (OpDivs), as well as various staffing levels (general staff, managers, executives within the OpDivs. Within the Business Intelligence Support Team there are administrators who perform user and security administration for the system) are given access to various pre-programmed or “canned” reports and are granted the capability to build custom (ad-hoc) reports via a user –friendly simplified representation of data.

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

BIIS is a HHS-wide data warehouse that contains personnel, time and attendance, payroll, HR, learning, workflow, budget, workmen's compensation, and Equal EEO information.

The BIIS data warehouse contains Personally Identifiable Information (PII) about employees used to conduct internal activities such as:

(i) Reporting - generating reports for each of the types of data BIIS contains.
(ii) Analyzing - the data contained in the reports can be used by managers to analyze subjects such as retirement trends and employee counts.
(iii) Succession planning - planning for how an organization replaces staff that retires or leaves the organization for some other reason.
(iv) External organization information requests - required recurring reports and ad hoc requests for authorized external organizations including:

The Office of Personnel Management (OPM) - Quarterly Headcount and Full Time Equivalent (FTE) (113A & G), annual Reemployed Annuitant, annual Student Loan Repayment, ad hoc reports as requested: Office of Management and Budget (OMB) - Quarterly 113G, ad hoc reports as requested

The White House - ad hoc reports as requested: Congress - Annual Department-Wide Pension Benefits Report; ad hoc reports as requested for Congressional Inquiries; General Accounting Office (GAO) - ad hoc reports as requested for audits; Equifax Workforce Solutions - Receives recurring Personnel and Payroll data for the Department's Employment and Verification System; The Work Number; Government Retirement & Benefits, Inc. (GRB) - Receives recurring Personnel and Payroll data for the Department's Employee Benefits Information System (EBIS).

BIIS contains thousands of data elements too many to name. However, the functional areas covered by these data elements are, social security numbers (SSNs), names, dates of births, addresses (mailing & email), phones, military & employment status, financial account information, payroll information, health benefit & life insurance plan selections, and other benefits information.

The SSN is integral to processing payroll data, making it a required data element for payroll reporting in BIIS.

Aside from the PII data that exists in BIIS that comes from the source systems mentioned above, BIIS uses PII in the process of creating user accounts (name, HHS Identification Number (HHSID), email address)

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

BIIS is a consolidated enterprise reporting system that collects, tracks, routes, maintains, and reports personnel, pay, attendance/leave, HR, learning, workflow, budget, workmen's compensation, and Equal EEO information relating to all HHS employees. It contains thousands of data elements too many to name. However, some of these data elements are: social security number (SSNs), name, date of births, address (mailing & email), phone number, military & employment status, financial account information, payroll information, health benefit & life insurance plan selections, and other benefits information.

BIIS is used to access HHS wide personnel (EHRP), Time and Attendance (ITAS), Recruitment (EWITS), Payroll (DFAS), Learning (LMS), Budget, Workmen's Compensation, and EEO/Diversity and Inclusion Information. HHS employees can also access various pre-scripted reports or create ad-hoc reports.

External organization information requests - required recurring reports and ad hoc requests are provided for authorized external organizations including:

The Office of Personnel Management (OPM) - Quarterly Headcount and Full Time Equivalent (FTE) (113A & G), annual Reemployed Annuitant, annual Student Loan Repayment, ad hoc reports as requested:

Office of Management and Budget (OMB) - Quarterly 113G, ad hoc reports as requested

The White House - ad hoc reports as requested:

Congress - Annual Department-Wide Pension Benefits Report, ad hoc reports as requested for Congressional Inquiries; General Accounting Office (GAO) - ad hoc reports as requested for audits; Equifax Workforce Solutions - Receives recurring Personnel and Payroll data for the Department's; Employment and Verification System, The Work Number; Government Retirement & Benefits, Inc. (GRB) - Receives recurring Personnel and Payroll data for the Department's Employee Benefits Information System (EBIS);

--'Ad hoc reports as requested' was added to those external agencies who can request ad hoc reports as necessary.

Examples of information being shared are: SSNs, names, dates of births, and addresses.
BIIS is a data repository from which data is extracted to create reports as well as data files. Canned reports are available to users at their convenience. Some reports and data files are scheduled for recurring delivery to users, at their request. Reports to both internal and external parties (named above) are generated monthly, quarterly, annually, upon request, and at the convenience of the user if they have access to the canned reports. BIIS uses PII in the process of creating user accounts (name, HHSID, email address).

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

E-Mail Address

Mailing Address

Phone Numbers

Financial Accounts Info

Military Status

Employment Status

Payroll information, health benefit plan selection, life insurance plan selection, and other benefits

HHS User Credentials

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

Employees

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

Vendor/Suppliers/Contractors

The only information included about contractors is name, e-mail address, and organization supported.

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

PII is used by developers and customers to generate reports, data files, and dashboards.

Internal and external customers log into BIIS via the HHS Access Management System (AMS), the Department's Single Sign-On (SSO) solution, for secure access to various pre-programmed ("canned") reports. However external customers would only be able to access BIIS if they were inducted into the Department's Active Directory/Smart Card Management System (SCMS) or by receiving that information from someone who does have access to BIIS, via secure email or file transmission methods.

BIIS also provides customers the opportunity to build their own custom ("ad hoc") reports via a user-friendly function that uses an easily-understandable representation of the data that BIIS can access. Developers generate various canned and ad hoc reports for internal and external customers especially in circumstances when customers need reports that are of a complex nature or when there is no existing canned report that meets their needs. Internal customers consist of all of the HHS Operating Divisions (OpDivs) and the Office of the Inspector General. External customers are OPM, OMB, The White House, Congress, GAO, Equifax Workforce Solutions, and GRB.

PII is not included in reports unless required, and access to PII is not granted to users who are not authorized to view PII.

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

None.

Describe the function of the SSN.

In BIIS, the SSN is primarily used to identify distinct individuals, especially in the case of the payroll data, where SSN is the unique identifier for employees.
And, SSNs are only used in reports where the data is being compared to data from DFAS, because DFAS uses SSN as employees' primary key.

Cite the legal authority to use the SSN.

This information is provided pursuant to 5 United States Code (U.S.C.) 552a (Privacy Act of 1974) for individuals supplying information for inclusion in a system of records. Executive Order (E.O.) 9397 and 31 U.S.C. 7701(c) (2) authorize the collection of the SSN. The former is the Executive Order noting that the SSN is to be used for various official government purposes, including as the Taxpayer Identification Number (TIN), and the latter states "The head of each Federal agency shall require each person doing business with that agency to furnish to that agency such person's taxpayer identifying number."

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

The implementation of this system, including activities such as the collection of PII necessary for operating it, are authorized by 5 U.S.C. 301. 42 U.S.C § 3502 creates the Office of the Assistant Secretary for Administration (ASA) at HHS, and among the duties delegated to the ASA are oversight of these services, which are necessary to developing and maintaining a workforce.

31 U.S.C. 66a; 5 U.S.C. 5501 et seq., 5525 et seq., 5701 et seq., and 6301 et seq.; Executive Order 9397; Pub. L. 100–202, Pub. L. 100–440, and Pub. L. 101–509

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.

09-90-0018 Personnel Records in Operating Offices

OPM/GOVT-1 General Personnel Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

There is no applicable OMB information collection approval number and expiration date for this item.

Is the PII shared with other organizations?

Yes

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

Within HHS

PII is only made available to those authorized to have access to such information. Those persons are allowed to access PII for staff at their organization level and below, within their OpDiv. Authorized personnel at the Department level can access PII for employees throughout the Department.

Other Federal Agencies

Only DFAS has direct access to BIIS. They access payroll and personnel reports as aids in resolving payroll issues. DFAS, part of the US Department of Defense, is HHS' payroll services provider. Authorized DFAS staff access BIIS to obtain information used to resolve payroll issues.

For all other external agency requests, an HHS staff member generates the reports and/or files that are sent to the external agency. In some cases the reports and/or files may contain PII, but external agencies outside of DFAS do NOT have direct access to BIIS. These reports and/or files are provided only if there is a legal basis to do so.

Private Sector

The following external private sector organizations receive information from BIIS that contains PII:

Equifax Workforce Solutions - receives personnel and payroll information. Equifax Workforce Solutions maintains an HHS approved system that provides automated employment verification for HHS Employees.

GRB - receives personnel, payroll, and time and attendance information. GRB maintains Employee Benefits Information System (EBIS), an HHS approved system that provides employees various benefits information (i.e. retirement and annuity).

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

Interconnection Security Agreements (ISAs)and/or Memorandums of Understanding (MOUs) exist for all BIIS data files (interfaces) provided to customers throughout all HHS OpDivs, as well as to the external customers (ie OMB, ..etc) named previously in this document.

Describe the procedures for accounting for disclosures.

Disclosures from this system are unlikely to be made, except in furtherance of the primary purpose of the system. If any nonstandard disclosures were to be made for any unanticipated reason, such that the disclosure was not a routine use, the system owner would maintain a record in a designated file to document who made the request; exactly what information on each individual was provided; and the date of the disclosure.

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 notification process in place for the Federal employee information that BIIS receives from the previously mentioned source systems.

BIIS uses PII in the process of creating user accounts (name, HHSID, email address). Individuals are required to complete a Request for Access form prior to gaining access to the system, and this information is collected on that form. When individuals indicate interest in accessing BIIS, they are told that completion of the form is required for access.

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.

BIIS uses PII in the process of creating user accounts (name, HHSID, email address). Individuals are required to complete a Request for Access form prior to gaining access to the system, and this information is collected on that form. When individuals indicate interest in accessing BIIS, they are told that completion of the form is required for access. If individuals do not complete the form, they are not granted access to the system.

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

Individuals would be notified directly of major system changes that affect their rights or interests, but no such changes are anticipated. Additionally, because this system is subject to the Privacy Act a System of Records Notice (SORN) is required to be revised describing some of the ways the records will be used within the agency and some of the reasons why the records may be disclosed to parties outside the agency. If a system changes in a way that will conflict with the SORN, a new or revised SORN may need to be published 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.

BIIS contains data for federal civilian and Commissioned Corps HHS employees. All formal and informal federal procedures are available for queries and concerns. Individuals may request assistance from supervisors, human resource offices, Help Desk lines, or Information Security Officers, all of which would ultimately lead to correction or mitigation.

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

There is no process in place for periodic reviews of PII in BIIS that is received from source systems. Because the system obtains its federal employee information from source systems it relies on the integrity, availability, accuracy and relevancy of those systems' information.

BIIS uses PII in the process of creating user accounts (name, HHSID, email address). User information is reviewed periodically to determine if individuals have left the department or transferred to another organization. The individual's account is deleted, unless he/she is moving to another organization and the new organization requests continued access with the appropriate data access modifications prior to the move (a new access request form must be submitted).

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

Users:

Users in each OpDiv request access to obtain information related to the work they do either from an Executive Management standpoint, or at lower staff levels across the functional areas the data in BIIS covers.

Administrators:

BIIS Administrators require access to properly assign and monitor data access, create accounts, verify security clearance level 5 or greater prior to providing access, and to report violations if necessary.

Developers:

Developers require access so that they can run reports and ensure their accuracy. Access also helps when assisting customers with troubleshooting issues and or questions about reports and data files.

Contractors:

Contractors serve as Developers and Administrators, so they require access for the same reasons stated for Administrators and Developers above.

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

Access is restricted using an authorization process. Only privileged users with administrative rights can access 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.

Access rights are determined by need to know basis when the user requests access. An annual recertification process is conducted to make sure user roles have not changed.

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.

Information Systems Security Awareness and Privacy Awareness trainings are required annually. Rules of behavior must be acknowledged and signed before access is granted.

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

PII restrictions are covered as part of BIIS recurring training sessions held to instruct users on how to access and build reports.

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.

Records are retained and disposed of in accordance with National Archives and Records Administration's (NARA) General Records Schedule 2 (GRS 2), “Payrolling and Pay Administration Records,” which prescribes retention periods ranging from as short as a few months or years to as long as 56 years. When an employee is separated, leave records are incorporated into the Official Personnel File (OPF) maintained by the servicing personnel office (SPO), and payroll retirement information is transferred to the Federal Retirement Records Center in Boyers, Pennsylvania. The OPF is forwarded to the new employing agency by the SPO. These procedures are in accordance with U.S. Office of Personnel Management policies and procedures.

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

The following administrative, technical, and physical controls are in place for BIIS:
Administrative Controls:
System security plan
Contingency (or backup) plan
File backup
Backup files stored off-site
User manuals
Security Awareness
Training
Contractor Agreements
Least Privilege Access
PII Policies

Technical Controls:
Single Sign On (SSO)
User Identification and Passwords
Firewall
Encryption
Intrusion Detection System (IDS)

Physical Controls:
Guards
Identification Badges
Key Cards