



Privacy Impact Assessment for
**Benefits Financial Management
System (BFMS)**

January 31, 2023

Contact Point

Erica Roach
Deputy Chief Financial Officer
Office of the Chief Financial Officer

Reviewing Official

Kellie Cosgrove Riley
Senior Agency Official for Privacy



Abstract

The Benefits Financial Management System (BFMS) is a group of seven common applications that provide a means for the Office of Personnel Management's (OPM) Office of the Chief Financial Officer (OCFO) to manage and administer individual financial transactions. Of those seven applications, six are internal solutions and one is a Commercial Off the Shelf (COTS) product. This group of common applications provides services to the OCFO/Trust Funds program and resides on the OPM mainframe. The information in BFMS supports the creation of financial reports and financial statements on a monthly or yearly basis for internal reconciliation purposes by the OCFO, and for the annuitants and Federal employees who conduct business transactions. This Privacy Impact Assessment is being conducted because three of the systems/utilities making up BFMS collect, maintain, and use personally identifiable information about individuals for certain financial transactions.

Overview

The Office of the Chief Financial Officer (OCFO) uses the Benefits Financial Management System (BFMS) to manage and administer the Office of Personnel Management's (OPM) financial responsibilities and accounting for the Civil Service Retirement Fund, the Federal Employees' Group Life Insurance (FEGLI) program, the Civil Service Retirement System (CSRS), the Federal Employees Retirement System (FERS), the Federal Employees Health Benefits (FEHB) program, and the Retired Federal Employees Health Benefits (RFEHB) Program. BFMS is a group of common applications that resides on the OPM mainframe and supports the creation of financial reports and financial statements on a monthly or yearly basis for internal reconciliation purposes by the OCFO and for the annuitants and Federal employees who conduct business transactions with OPM. The seven applications that make up BFMS are:



1. Automated Voucher Control Log (AVCL). AVCL enables an OPM user to initiate, enter, update, cancel and make an inquiry on any voucher (invoice) over a ten-year fiscal period. This provides the user with complete control of the vouchers (invoice) and log from start to finish. Retirement Services sends the voucher details to the CIO Production Control team which in turn sends the details to Treasury electronically.
2. Bureau of Retirement Head Count (BRHC). BRHC is used to produce the Semiannual Headcount report, which provides a snapshot at a given point in time of all enrollees in the FEHB Program, the FEGLI Program, and both Federal Retirement systems (CSRS and FERS).
3. Payroll Office Master File (POMF). POMF contains a master list of agency payroll and health benefit reporting offices and is used by OPM to identify valid payroll offices and key personnel. The information in the application includes payroll and health benefit office numbers, names, addresses, and phone numbers of key contacts for the agency and/or office.
4. 2812 Application (Financial Management Collection Deposit (FMCD) 2812 Application). FMCD2812 is used by all agencies, cross-services, retirement payroll offices, and non-Federal organizations with employees entitled to Federal benefits to report aggregated data of FERS, CSRS, FEGLI, and FEHB withholdings and contributions.
5. Non-Periodic Payment Application (NPPA). NPPA is used to support OPM's Retirement Services functions and operations in the administration of retirement benefits provided to beneficiaries, annuitants, and survivors. NPPA is used to provide inquiries on the payment status of annuitants and to generate the information needed for OPM to prepare the Internal Revenue form 1099R from the NATS application. NPPA receives refund and lump sum death benefits information for tax reporting purposes. Inquiries include research in case a payee claims they did not receive a payment; mark a payment as cancelled if returned by Treasury; track a 1099R if payee claims they did not receive one; rarely, a payee contacts OPM regarding an inquiry from the IRS and OPM needs to show they did



receive the payment (e.g., an estate executor may have not reported the payment or filed the estate's tax return).

6. United States Postal Service Application (USPSA). USPSA creates billing data for the US Postal Service (USPS) to identify their share of the cost for Life Insurance and Health Benefits. The USPS is required to pay the government share of benefits for annuitants and survivors. In July 1971, the USPS became a quasi-government agency, and offered its employees the opportunity to enroll in the benefits programs administered by OPM and offered to Federal employees, such as the FEHB Program and the Federal Employees Group Life Insurance Program. USPS is responsible for the government share of the costs of these benefits. USPSA provides USPS with the number of USPS annuitants and survivors and a dollar amount for the government share of benefits to be collected each month for the trust funds. A bill is sent to USPS from the OPM OCFO and a file is sent to verify the bill.
7. Voluntary Contributions (VC). The VC application is used primarily by OCFO staff to record when employees covered by CSRS exercise their option to deposit additional money into their existing retirement contributions to increase the amount of their future annuity. The application also processes the re-deposit of money originally placed into the Trust Fund and subsequently withdrawn.
8. The services provided by the Federal Financial System (FFS), formerly a component of BFMS, have now been transferred to the Department of Treasury's Administrative Resource Center Integrated Oracle Solution. FFS is considered a Trust Funds System and part of the group of common applications that provides a means for the OCFO to manage and administer financial transactions of Trust Funds operations. More information can be found in OPM's Privacy Impact Assessment, Trust Fund Systems, published on OPM's web site.



Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Several statutes and other authorities support the collection of the information contained in BFMS. These include 31 U.S.C., Subtitle II, which defines the budget process and describes the method for establishing and accounting for an agency's Federal budget; and 31 U.S.C., Subtitle III, which describes the Federal financial management requirements and responsibilities to record accounting activities related to debt, deposits, collections, payments, and claims and to ensure effective control over, and accountability for, assets for which the agency is responsible.

Several other Federal financial mandates and legal authorities that govern financial management systems also support the collection of the information in BFMS. These include The Chief Financial Officers Act of 1990, Public Law 101-576, and the Federal Financial Management Improvement Act (FFMIA) of 1996, Public Law 104-208, as well as guidance issued by the Office of Management and Budget: OMB Circular A-123, Management's Responsibility for Internal Control; OMB Memorandum 16-11, Improving Administrative Functions Through Shared Services (May 2016).

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The relevant SORNS are OPM Internal 23, Financial Management Records and OPM Internal 5, Pay, Leave and Travel Records.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes, a system security plan for BFMS has been completed.



1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. The retention schedule applicable to the records in BFMS is GRS 1.1, Item 010, which requires records to be disposed of six years after final payment or cancellation, or longer if required for business use.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information contained in BFMS is not subject to the requirements of the PRA as BFMS collects information from Federal agency financial management applications and not directly from individuals.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

BFMS collects, uses, disseminates, or maintains, the following information within each of its seven applications:

1. Automated Voucher Control Log (AVCL). This application contains no sensitive financial data or personally identifiable information. AVCL is used by OCFO/Trust Funds Management to support preparation of new benefit payment vouchers for transmittal to the Department of the Treasury and, additionally, for tracking and controlling these payment vouchers between OPM and Treasury. Vouchers are created manually, and then entered into the AVCL. The system allows on-line entry, update and cancellation, and on-line inquiries. At entry, the system automatically generates the voucher number and date. After the voucher is received and processed by Treasury, AVCL is updated on-line by the user to reflect the status change.
2. Retirement Head Count (BRHC). This application contains non-sensitive financial data, including payroll office number and dollar amount. BRHC



dollar amounts are based on the withholding and contribution at a payroll office number level for a specific ALC. An ALC can have multiple payroll offices.

3. 2812 Application (FMCD). This application does not contain any sensitive information or PII. FMCD2812 is used to capture all agencies, cross-services, retirement payroll offices, and non-Federal organizations with employees entitled to Federal benefits to report aggregated data of FERS, CSRS, FEGLI, and FEHB withholdings and contributions. This is used primarily by OCFO with no outside OPM access.
4. Non-Periodic Payment Application (NPPA). This application contains sensitive financial information and PII. NPPA collects and maintains records containing the following types of information about individuals: full name; Social Security number (SSN); Mailing Address; Date of Birth; and bank account information. The application records individual payments separate from the recurring annuity roll payments.
5. Payroll Office Master File (POMF). POMF does not contain any sensitive financial information or PII. The information in the application includes payroll and health benefit office numbers, names, addresses, and phone numbers of key contacts for the agency and/or office.
6. United States Postal System Application (USPSA). This application contains sensitive financial information and PII. The USPSA is used to provide billing information to the United States Postal Service and the application collects and maintains records containing the following types of information and individuals: Full Name; Social Security number (SSN); and Date of Birth.
7. Voluntary Contributions (VC) -. PII Data Exists. The VC application collects and maintains records containing the following types of information associated with individuals: full name; Social Security Number (SSN); Mailing Address; Date of Birth.



2.2. What are the sources of the information and how is the information collected for the project?

BFMS collects information from Federal agency financial management systems and not directly from individuals. General Ledger information is received electronically from other OCFO Applications including Voluntary Contribution, Service Credit, Account Control File Application, and the Financial Management Collection Deposit Application. Some of the information in the system is derived from the Departments of Labor and Treasury.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4. Discuss how accuracy of the data is ensured.

BFMS receives data through automated interfaces and by using manual entry. The information maintained in BFMS is primarily received from other external systems. These source systems generally gather the information directly from agencies, vendors, and other commercial providers and as such are considered to be accurate. In addition, BFMS has various internal controls and procedures to ensure accuracy of the data. For instance, the majority of data in BFMS is received through automated system interfaces; the built-in system edits and configuration increases data accuracy by minimizing data entry errors. Before uploading to BFMS, the source data is also automatically evaluated for errors (e.g., file format, duplicate records, incorrect financial data), and if errors are found, BFMS will not accept the record(s) and will generate an error log that must be reviewed and reconciled by a user in consultation with the source system or provider. Once reconciled, the record is re-submitted to BFMS as part of the next automated transmission. Supervisory verification is put in place for all transaction postings and payment information.



2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that PII will be unnecessarily collected and maintained in BFMS.

Mitigation: BFMS has mitigated this risk by establishing effective policies to avoid unnecessary collection of PII and to redact PII if it is collected inadvertently. In addition, the Social Security number and bank account number is masked and transmitted via secure VPN connections so that its exposure is limited.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The Benefits Financial Management System uses the information, depending upon the application, as follows:

1. Automated Voucher Control Log (AVCL). AVCL is used by OPM's Retirement Services (RS) and the Office of the Chief Financial Officer (OCFO) to support preparation of new benefit payment vouchers for transmittal to the Department of the Treasury and, additionally, for tracking and controlling these payment vouchers between OPM and Treasury. Vouchers are created manually based on a signed supervisory authorization memo to enter information into the AVCL. The application allows on-line entry, update and cancellation, and on-line inquiries by OCFO employees. At entry, the application automatically generates the voucher number and date. After the voucher is received and processed by Treasury, AVCL is updated on-line by the OCFO user to reflect the status change.
2. Retirement Head Count (BRHC). BRHC provides a snapshot at a given point in time of the number of enrollees in the Federal Employees Health Benefits Program, the Federal Employees Life Insurance Program, and the Retirement Applications (CSRS & FERS). The Headcount is performed



twice yearly and is based on 2812 application aggregate data reported by each payroll office for the first payroll paid during the months of March and September.

3. 2812 Application. The 2812 Application processes collections from employees who participate in the Government-wide Life Insurance, Health Benefits, or Retirement programs and transferred to the Retirement and Insurance Transfer System (RITS). The data is collected through different sources such as RITS, OPM's Account at Treasury (CIR), Lockbox and Pay.gov, and via manual checks. This interfaces to the appropriations account in Administrative Resource Center (ARC) Integrated Oracle Solution (AIOS).
4. The Non-Periodic Payment Account Application (NPPA). NPPA is used to load, edit, record, maintain and report contributions, refunds and lump sum payments that are not processed through the monthly cycle payment process.
5. The Payroll Office Master File (POMF). This application is a repository of information of all the Federal Payroll Offices that submit monies to OPM for Retirement, Health Benefits, and or Life Insurance. The POMF application contains a master list of agency payroll and health benefit reporting office numbers, names, addresses, phone numbers, and contacts. It is used to identify valid payroll offices, generate address labels for payroll office mailings, and provide contacts for claims adjudication and reconciliation purposes.
6. United States Postal System Application (USPSA). USPSA creates billing data for the United States Postal Service to identify their share of the cost for life insurance and health benefits. This application provides information for all annuitants and survivors of the United States Postal Service who have health benefits and life insurance and also provides the number of Office of Workers Compensation Programs (OWCP) annuitants with a dollar amount for the government share of benefits to be collected



each month for the Trust Funds. A bill is sent to the United States Postal Service from the OCFO. Files are sent to USPS to verify the bill.

7. Voluntary Contributions (VC). VC is used to record CSRS employees' requests to make additional contributions to be added to their annuity.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

Data in BFMS is not used to conduct electronic searches, queries or analyses to discover or locate a predictive pattern or anomaly.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

Yes. In addition to OCFO, Retirement Services controls the Non-Periodic Payment Account (NPPA) and is responsible for assigning roles and responsibilities within NPPA. The application is used to maintain and report on refund and lump sum payments that are not processed as part of the monthly annuity roll payment cycle.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that an unauthorized user will access the system or that an authorized user will access the system for an unauthorized purpose.

Mitigation: This risk is mitigated by implementing strict procedures for individuals to obtain access and limiting that access consistent with their roles.



Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Individuals do not have direct access to the system and therefore the system itself does not provide any notice to the individuals whose information it contains. Individuals do receive information about BFMS via publication of this PIA and receive notice concerning how their information will be used via Privacy Act statements on any forms they are required to complete and via the SORNs identified in Section 1.2.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals do not have direct access to the system and therefore the system itself does not provide any notice to the individuals whose information it contains. There is no opportunity for individuals to consent to having information included in the system.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know that their information is being collected, used, and maintained in BFMS.

Mitigation: This risk is mitigated through publication of this PIA and, while not directly referencing BFMS, through the Privacy Act statements on relevant forms that explain why information is being collected and how it will be used, as well as through publication of applicable SORNs.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

The records in BFMS are maintained according to the retention schedule identified in Section 1.4, which requires that the records be destroyed 6



years after final payment or cancellation, but longer retention is authorized if required for business use.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information in BFMS will be retained for longer than is necessary to achieve the business purpose for which it was collected.

Mitigation: This risk is mitigated by adhering to the applicable records schedule, which addresses the business need to retain the information.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information in BFMS is shared with the Department of the Treasury's Financial Management System (FMS TWAI). The purpose of this connection is to reduce government operating costs, providing greater functionality, and improving efficiency in financial management.

Information is also exchanged with the Department of Labor so that OPM can receive workers' compensation data, to include case management, medical payment, compensation payment, and chargeback related information at regular intervals.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing described above is compatible with the original purpose for which the information was collected, namely, to perform financial management functions to support OPM business operations.

6.3. Does the project place limitations on re-dissemination?

Yes, re-dissemination of BFMS information is subject to the terms in stated and signed contracts and interagency agreements.



6.4. Describe how the project maintains a record of any disclosures outside of OPM.

Records of information disclosed outside of OPM are maintained through interface logs upon integration with the applications identified in this PIA. For example, OPM uses the payment schedule dates from when batch payment files are transmitted to Treasury to track disclosures of BFMS data outside of OPM. By recording the payment schedule date from the batch file, BFMS records the disclosure of the associated records and data.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be disclosed outside of OPM for a purpose that is not consistent with the purpose for which it was originally collected.

Mitigation: This risk is mitigated through the use of appropriate security protocols so that information is accessible only by the intended recipient and by disclosing information consistent with the purpose for which it was originally collected.

Privacy Risk: There is a risk that information properly shared outside of OPM will be further disseminated for a purpose that is not consistent with the original purpose for sharing nor with the original purpose for which it was collected.

Mitigation: This risk is mitigated by ensuring that the sharing is subject to written agreements that define the purposes for which the information is shared, prohibits additional uses, and appropriately limits any onward sharing with third parties.



Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

Individuals do not have direct access to BFMS. However, they may request access to records about themselves by following the procedures outlined in the applicable SORN identified in Section 1.2.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals who access their records may request correction of any inaccurate or erroneous information by submitting a request to correct the data via the procedures outlined in the applicable SORN identified in Section 1.2.

7.3. How does the project notify individuals about the procedures for correcting their information?

The procedures for submitting a request to correct information are outlined in the OPM/Internal 23 Financial Management Records System of Records..

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be able to access their information and request appropriate amendment to inaccurate or incomplete information.

Mitigation: This risk is mitigated by providing individuals with an appropriate opportunity to request access to and amendment of their records as outlined in applicable SORNs.



Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

Only users who have a need to access the system, as determined by their supervisor and the system security office are granted access. In addition, audit logs are kept which track access to and disclosures from the system.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM personnel are required to take IT Security and Privacy awareness training annually.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

A Federal supervisor or the security officer assigned to the system must approve any user's access via the OPM IT Access Request form. In addition, all users must have a background investigation and complete annual training before being granted access.

Each user account is assigned specific roles with a defined set of privileges. BFMS system administrators can elect to assign all the privileges for a given role or can select only certain privileges to assign. Access is limited to OPM employees who have a need to access the system based on their roles in support of financial administration and management operations at OPM. To gain access to BFMS, users must complete the system-specific user training and submit a request for system access to the authorized point of contact in their program office. The roles and privileges assigned to a particular user are predetermined depending on the user's function.



8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The BFMS ISSO reviews and updates the ISAs every three years. In some instances, the partner agencies require OPM/CIO to conduct an annual review of the ISAs & MOUs. After ISSO review and updates the ISA document then it is forwarded to OPM CISO for signature. The system owner, ISSOs, Technical POC, and CISOs from each organization reviews the ISAs before it is finalized.

Responsible Officials

Erica Roach
Deputy Chief Financial Officer
Office of the Chief Financial Officer

Approval Signature

Kellie Cosgrove Riley
Senior Agency Official for Privacy