Privacy Impact Assessment for

Trust Funds Systems

September 21, 2022

Contact Point

Erica D. Roach
Acting Deputy Chief Financial Officer
Office of the Chief Financial Officer

Reviewing Official

Kellie Cosgrove Riley
Senior Agency Official for Privacy

Abstract

The Office of Personnel Management's Office of the Chief Financial Officer has embarked on a Trust Funds Modernization (TFM) Program to enhance the administration and the financial oversight for the employee and annuitant Trust Funds for retirement, health benefits, and life insurance. The TFM involves stand-alone systems, as well as a series of other systems interfacing into the Department of the Treasury's Administrative Resource Center Integrated Oracle Solution. These systems, collectively referred to as "Trust Funds Systems," is a group of common applications that provide a means for the OCFO to manage and administer financial transactions of Trust Funds operations. The information in the Trust Funds Systems supports the creation of financial reports and financial statements on a monthly or yearly basis for internal reconciliation purposes by the OCFO. This Privacy Impact Assessment is being conducted because the Trust Funds Systems collect, maintain, and use personally identifiable information about individuals for certain financial transactions.

Overview

The Office of the Chief Financial Officer (OCFO) uses the Trust Funds Systems to manage and administer the Office of Personnel Management's (OPM's) financial responsibilities and accounting for the Civil Service Retirement and Disability 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. OCFO has embarked on a ss Modernization (TFM) Program to enhance the administration and the financial oversight for the employee and annuitant Trust Funds for retirement, health benefits, and life insurance. OPM is implementing a two-release migration strategy to achieve the target state, which includes the migration of Trust Funds data and functions from the OPM's legacy Federal Financial Management System

(FFS) and FMCD2812 systems to the Department of the Treasury's shared services environment. Release 1 replaces FFS and the FFS Investment Subledger module with Treasury's Administrative Resource Center (ARC) Integrated Oracle Solution (AIOS). After Release 1, OPM will access the AIOS for the core financial management functions: Receivable Management, Payment Management, Debt Management, Budget Execution, and Financial Reporting and Reconciliations. However, OPM will continue to operate the FMCD2812 for Trust Funds Account Management and Trust Funds Reporting functions. As part of the first release of this migration, OPM programmatic systems will interface with the AIOS, rather than FFS, to automate the summary and detailed transactions postings.

The Trust Funds Systems is a group of applications that supports the creation of financial reports and financial statements on a monthly or yearly basis for internal reconciliation purposes by the OCFO. The program involves the following systems:

- Treasury ARC Integrated Oracle Solution (AIOS): In Release 1, the AIOS replaces FFS as the core Trust Funds financial system. This includes accounts receivable, accounts payable, purchasing, Federal administration, and general ledger functionality. This system will contain individual debtor information, including the Social Security number (SSN).

- 2812 Application (Financial Management Collection Deposit (FMCD2812): FMCD2812 is an existing OPM system. FMCD2812 processes collections made by all agencies from their employees who participate in the government-wide life insurance, health benefits, or retirement programs. Agencies, cross-services, retirement payroll offices (and non-Federal organizations with employees entitled to Federal benefits) report FERS, CSRS, FEGLI, and FEHB withholdings and contributions electronically through the Retirement and Insurance Transfer System (RITS), via SF-2812, or through OPM's lockbox via the FMCD2812 Initial Entry

(FMCD2812IE). This system will remain after Release 1. FMCD2812 will have three one-way interfaces into Treasury Oracle Solution.

- Payroll Office Master File (POMF): POMF is an existing OPM system. The POMF data will be migrated into the Treasury's AIOS. This data contains a master list of agency payroll and health benefit reporting offices and is used by OPM to identify valid payroll offices.

- OPM Programmatic Systems: The following OPM systems have one-way interfaces into the AIOS: Accounting Control File System (ACFS); Lump Sum System (LSUM); Refund System (RFND); Annuity Roll Processing System (ARPS); Check Cancellation System (CHCN); Non-Receipt/Recertification System (NRRC); and Service Credit Redeposit Deposit System (SCRD).

- Department of Labor (DOL) Office of Worker's Compensation (OWCP) Data: This data has one-way interfaces into the AIOS.

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 the Trust Funds Systems. 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 the Trust Funds Systems. These include the Chief Financial Officers Act of 1990 (Public Law 101-576); the Federal Financial Management Improvement Act (FFMIA) of 1996 (Public Law 104-208); and guidance issued by the Office of Management and Budget (OMB): OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control; OMB Memorandum-17-22, Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce; and OMB Memorandum-19-16, Centralized Mission Support Capabilities for the Federal Government.

The authority to collect and use SSNs is provided by Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

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

OPM Internal 23, Financial Management Records.

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

Yes. The Department of Treasury has issued an Authority to Operate the Administrative Resource Center (ARC). OPM has an Authority to Use ARC that was signed on September 16, 2022.

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 the Trust Funds Systems 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 the Trust Funds Systems is not subject to the requirements of the PRA as the Trust Funds Systems collects information from Federal agency financial management applications and not from members of the public.

Section 2.0. Characterization of the Information

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

The Trust Funds Systems collects, uses, disseminates, or maintains, the following information:

AIOS: AIOS contains sensitive financial data, and off-roll debt individual record information. The application provides audit trails, transaction processing, archiving, accruals, closings, consolidations, and general ledger analysis and reconciliation functions.

FMCD2812: 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. No individual information is collected. This is used primarily by the OCFO.

POMF: POMF does not contain sensitive financial information and limited PII in the form of business contact information. 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.

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

The Trust Funds Systems 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.

The Trust Funds Systems receives data through automated interfaces and through user manual entries. The information maintained in the Trust Funds Systems is also received from OPM programmatic systems. These source systems generally gather the information directly from agencies and vendors and as such are considered to be accurate. In addition, AIOS has various internal controls and procedures to ensure accuracy of the data. For instance, the majority of data in AIOS is received through automated system interfaces; the built-in system edits and configuration increases data accuracy by minimizing data entry errors. Before uploading to AIOS, the source data is also automatically evaluated for errors (e.g., file format, duplicate records, incorrect financial data), and if errors are found, AIOS 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 the AIOS 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 the Trust Funds Systems.

Mitigation: The Trust Funds Systems 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 SSN and bank account number is masked and transmitted securely so that its exposure is limited.

Privacy Risk: There is a risk that the information in the system will be inaccurate and result in erroneous financial decisions that adversely impact individuals.

Mitigation: This risk is mitigated via the steps described in Section 2.4, above.

Section 3.0. Uses of the Information

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

The Trust Funds Systems uses the information, depending upon the application, as follows:

AIOS: As the new core Trust Funds financial system, AIOS includes accounts receivable, accounts payable, purchasing, Federal administration, and general ledger functionalities. These functionalities are used to manage debts and non-debt receipts; establish budgets and funds control levels, distribute funds, and monitor spending; create financial reports to comply with Federal and OPM reporting requirements; manage financial, post accounting transactions, and create journal vouchers; and record Trust Funds investments and related financial transactions.

FMCD2812: FMCD2812 processes collections from employees who participate in the government-wide life insurance, health benefits, or retirement programs and transferred to the 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 AIOS.

POMF: POMF 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.

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.

No.

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

No other OPM programs/offices other than OCFO have assigned roles and responsibilities in the system. AIOS is hosted on the Treasury's ARC shared services platform.

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 the Trust Fund Systems via publication of this Privacy Impact Assessment (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 SORN 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 the Trust Funds Systems.

Mitigation: This risk is mitigated through publication of this PIA and, while not directly referencing the Trust Funds Systems, 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 the applicable SORN.

Section 5.0. Data Retention by the Project

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

The records in the Trust Funds Systems are maintained according to the retention schedule identified in Section 1.4 of this PIA, which requires that the records be retained for six 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 the Trust Funds Systems 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 the Trust Funds Systems is on Treasury ARC’s Oracle Integrated Solution. The purpose of this connection is to reduce government operating costs, providing greater functionality, and improving efficiency in financial management across federal agencies.

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 the Trust Funds 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 the Trust Funds data outside of OPM. By recording the payment schedule date from the batch file, the Trust Funds 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 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 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. This risk is also 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 the Trust Funds Systems. 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 SORN Internal 23, Financial Management 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 SORN.

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 (Federal and contractors) are required to take the Cybersecurity and Privacy Awareness Training annually. Any OPM personnel who do not complete this mandatory training will have their IT accounts disabled.

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 ARC Oracle Access Request and OPM IT Request forms as required. In addition, all users must have a background investigation and complete annual Cybersecurity and Privacy Awareness Training before being granted access.

Each user account is assigned specific roles with a defined set of privileges. AIOS 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 AIOS, 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 Information System Security Officer reviews and updates the Interconnection Security Agreements every three years. In some instances, the partner agencies require OPM/CIO to conduct an annual review of the ISAs & MOUs. After the ISSO reviews and updates the ISA 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 D. Roach
Acting Deputy Chief Financial Officer
U.S. Office of Personnel Management

Approval Signature

Signed Copy on File with the Senior Agency Official for Privacy

Kellie Cosgrove Riley
Senior Agency Official for Privacy