Privacy Impact Assessment for the

Payment Processing Automation Initiative - Online Bill Payment (PPAI-OLBP)

June 3, 2020

Contact Point

Isaiah Waters

Financial Management Specialist | PPAI-OLBP Project Manager

System Planning & Development (SPD)

Financial Operations Management (FOM)

Office of the Chief Financial Officer (OCFO)

Reviewing Official

Kellie Cosgrove Riley

Chief Privacy Officer

Abstract

The Payment Processing Automation Initiative - Online Bill Payment (PPAI-OLBP) is an online, automated solution being implemented by the Office of Personnel Management's (OPM) Office of the Chief Financial Officer (OCFO) in order to streamline the current cash receipt process, reduce or eliminate manual business processes, and foster better information sharing across the agency. PPAI-OLBP aims to refine OPM's overall cash management practices by ultimately reducing paper-based collections and automating the receipt and initial processing of payments made to OPM. This Privacy Impact Assessment (PIA) is being conducted because PPAI-OLBP will collect, maintain, and disseminate personally identifiable information (PII) about federal employees, annuitants, and their families.

Overview

OPM serves as the chief human resources agency for the Federal government. In this capacity OPM directs human resources and employee management services, administers retirement benefits, and manages healthcare and insurance programs, among other mission objectives. OPM OCFO provides critical accounting and financial management services and reporting and is responsible for the financial leadership of the agency, including all OPM disbursements and accountability processes and management and coordination of OPM planning, budgeting, and analysis.

To enable agencies to meet their financial responsibilities, in 2018 the Department of the Treasury (Treasury) issued a 10-year vision for federal financial management focused on making improvements across four broad areas. At the heart of many of those improvements will be the modernization of financial management, to include technology advancements and expanded offerings. Associated with this technological vision is the Payment Processing Automation Initiative - Online Bill Payment (PPAI-OLBP), which implements an automated, online solution for Trust Funds payments. OPM and Trust Funds Management oversee the financial aspects of all the benefit programs OPM administers. Trust Funds payments within the scope of PPAI-OLBP include non-tax debts owed to the Federal

government, payments of life and health insurance premiums to OPM, along with voluntary payments towards an individual's retirement annuity. PPAI-OLBP provides added cost savings within OPM by reducing the receipt of physical checks and money orders by automating the receipt and initial processing of seven (7) types of payments made to OPM, including: 1) Reclamations, 2) Annuity Service Credit, 3) Manual Repay, 4) Direct Premium Life Insurance (DPLI), 5) Employee Service Credit, 6) Voluntary Contributions, and 7) Off-Roll Debt.

PPAI-OLBP provides an efficient and effective cash handling solution that leverages proven technology, improves transparency and accountability through increased standardization and the reduction of redundant processes, and enhances the processing of financial transactions between OPM and its customers (employees, annuitants, survivors). PPAI-OLBP will enable OPM to provide customers an online payment option by partnering with Treasury's Bureau of the Fiscal Service's (Fiscal Service) Credit Gateway. The Credit Gateway is a trusted and secure way for OPM and other Federal agencies to get their money from both the FedWire and Automated Clearing House (ACH) network. OLBP is also a convenient way for OPM's customers to use their own financial institution's website or mobile application to pay the Federal government electronically via an ACH credit. As collections are processed, transactional data is simultaneously sent to the Fiscal Service's Collections Information Repository (CIR). The CIR is a web-based tool that provides Federal agencies information on deposits and collections made from within the financial banking network. The CIR streamlines financial transaction information from all collections and settlement systems into one place, thus Federal agencies use CIR to get detailed and summary-level information on revenue they receive and to report collections data.

Currently, OPM customers receive a letter containing notification of payment due with instructions for making payments to OPM. Instructions will include the use of OLBP for making an online payment, as well as instructions for paying OPM with a personal check or money order. If the OPM customer does not recognize the notification of payment due, the letter includes OPM contact information (phone number and mailing address) for assistance (additional information regarding payments to OPM is available on opm.gov).

Notably, participation in OLBP is voluntary as OPM will continue to support the processing of paper-based collections. Upon the submission of an online payment, the customer (Payer) must agree to authorize the payment. It is assumed that the act of making a payment, whether via OLBP or paper, involves the sharing of the Payer's information with the receiving party (OPM).

Should an OPM customer choose to make a payment via OLBP, they must take steps at their financial institution to submit a payment, following their financial institution's process to establish and submit an online bill payment. Following the submission of an online payment, the CIR will receive the ACH payment information. As part of PPAI-OLBP, OPM will configure a System-to-System (S2S) connection with the CIR which will enable Treasury to securely transmit transactional data (including PII) to OPM automatically.

The implementation of PPAI-OLBP will enable OPM to automate the receipt and initial processing payments into various financial and retirement systems such as the Annuity Roll System (ARS), Benefits Financial Management System (BFMS), and Service Credit Redeposit and Deposit System (SCRD). These systems are vital to the benefits and financial management of the Federal workforce, annuitants, and their families. OPM will deliver enhanced services to customers by providing an additional payment option (OLBP), and the transactional data provided electronically from the Treasury coupled with automation with reduce the overall processing time of collections made by OPM.

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 authorities are relevant to the PPAI-OLBP project. These include authorities related to OPM's financial responsibilities, such as 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); the Chief Financial Officers Act of 1990, Public Law 101-576; the Federal Financial

Management Improvement Act (FFMIA) of 1996, Public Law 104-208; OMB Circular A-123 Management's Responsibility for Internal Control; OMB Memorandum 16-11, Improving Administrative Functions Through Shared Services (May 2016); and OMB Memorandum 13-08, Improving Financial Systems Through Shared Services. In addition, they include authorities related to administration of the Civil Service Retirement System (CSRS), 5 U.S.C. chapter 83, and the Federal Employee Retirement System (FERS), 5 U.S.C. chapter 84. In addition, Executive Order 9397, as amended by Executive Order 13478, is relevant to the collection and use of Social Security numbers.

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

Many of the records associated with the PPAI-OLBP that OPM receives ultimately are received and processed in various retirement and financial management systems. Those records that are included in retirement systems are covered by OPM CENTRAL-1 Civil Service Retirement and Insurance Records. The Office of the Chief Financial Officer will work with the Office of Privacy and Information Management to determine whether additional SORNs exist or are required that apply to these records.

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

Yes. System Security Plans (SSPs) were completed in conjunction with the Authority to Operate (ATO) packages for the relevant OPM information systems supporting PPAI-OLBP.

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

Yes. General Records Schedule (GRS) 1.1 Financial Management and Reporting Records, Item 10, applies to the records this system, as does DAA-0478-2017-0001-0001 for those records that become part of an individual's retirement file. which requires that the records be retained for 6 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.
Not Applicable.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.
PPAI-OLBP project collects, uses, and maintains Payer (customer) Name, Payer OPM-designated Account Number, Payment Type (Cashflow Name *and* Credit Gateway Account Number), Payment Settlement Date, Payment Amount, and Payment Trace Number.

2.2. What are the sources of the information and how is the information collected for the project?
The source of information for PPAI-OLBP is Treasury's Fiscal Service Collections Information Repository (CIR). CIR will transmit files daily to OPM via a secure data connection.

The data transmitted from CIR is initially generated in the OLBP network. The data is generated at the time a customer uses their financial institution website or mobile application to initiate an online payment to OPM.

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.
Instructions and data validation steps are provided to individuals to assist them in providing accurate data. If errors do occur, the system has processes in place to identify and resolve these errors.

Specifically, OPM provides detailed payment instructions to individuals for making payments to OPM. This is accomplished through updated payment notification letters that OPM sends to customers (payers) and via detailed

instructions and Frequently Asked Questions (FAQs)on the "How to Make a Payment" webpage on the opm.gov website.

The first step in validating the data occurs while the payer is entering information to make a payment via their financial institution's website or mobile application. Treasury's OLBP service enables OPM to implement custom data validation rules to the format of entered data and ensure a minimum level of information is provided by the customer. When validation rules identify an error, the customer is prompted to enter payment information several times, however a customer can force a payment that does not meet the data validation rules. Ultimately, the customer data entry error results in a paper check or "drop check" from the customer's financial institution to OPM. Upon receipt, OPM may process and deposit the drop check or return the check to the issuing financial institution (the drop check includes enough information to initiate a return of payment, if needed).

The second data validation step occurs after OPM receives the file from Treasury and prepares data for processing. Each payment is validated against OPM databases using the Payment Type, OPM-designated Account Number, and Name. Should a payment fail this validation step, it is flagged and a report is provided to the appropriate staff for investigation and, as appropriate, corrected and processed or returned to the customer.

In the meantime, any technical issues such as missing data files or data upload issues result in notifications to the relevant points of contact (POCs). OPM Office of the Chief Information Officer (OCIO) is tasked with troubleshooting and communicating any technical issues to the identified OCFO stakeholders.

Lastly, processed payments appear in reports that are used in daily reconciliation processes.

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

Privacy Risk: There is a risk that OPM will collect more information than is necessary to meet the business needs to adequately process a customer's payment to OPM.

Mitigation: This risk is mitigated in the development of a program that will parse out only the payment information that has been deemed pertinent to the application of payment.

Privacy Risk: There is a risk that the payment information received will not be accurate and OPM will be unable to correctly identify a payment and process said payment.

Mitigation: This risk is mitigated in the development of a program that will validate payment information and flag all payments that fail validation for investigation. Payments that cannot be manually validated will then be returned to the customer (payer).

Section 3.0. Uses of the Information

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

Payer (customer) Name, Payer OPM-designated Account Number, and Payment Type (Cashflow Name *and* Credit Gateway Account Number) are used as the means to identify the individual and properly align their payment to the correct account.

Payer OPM-designated Account Number, Payment Type (Cashflow Name *and* Credit Gateway Account Number), Payment Amount, and Payment Trace Number are used as the means to update the customer's OPM account with payment information.

Payment (settlement) Date, Payment Trace Number, and Payment Amount are used to issue a return to customers who made an erroneous payment to OPM.

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.

The project does not use technology to discover or locate a predictive pattern or an anomaly.

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

Within OPM, only OCFO and OCIO have assigned roles and responsibilities related to PPAI-OLBP business processes and technical support. OPM OCFO references summary reports for validation and accounting, showing both automatically processed payments and payments that have been flagged for error. Payments in an error state (tallied on an Error Log Report) are investigated and resolved (corrected or returned) following an established manual process.

OPM OCIO stores source files, resolves any technical issues related to uploading information to systems, oversees the daily operation and maintenance of related systems, and provides reports for OCFO stakeholders.

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

Privacy Risk: There is a risk that authorized individuals may use information obtained through the use of OLBP for unauthorized purposes or that unauthorized individuals may gain access to the information.

Mitigation: This risk is mitigated through access controls that limit access to only those with a need to know and only with access appropriate to their roles and responsibilities. In addition, user access information will be captured by audit logs. Access to information is further limited by ensuring data is transmitted between agencies via a secure connection, and only authorized individuals have access to the designated landing zone.

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.

OPM customers receive notification letters with instructions for making payments to OPM. Instructions include the use of OLBP for making an online payment, as well as instructions for paying OPM with a personal check or money order. It is at the sole discretion of OPM's customer as to how they wish to submit payment to OPM.

Upon the submission of an online payment, an individual must agree to authorize the payment. It is assumed that the act of making a payment, whether via OLBP or paper, involves the sharing of the payer's information with the receiving party. Additional information regarding payments to OPM is available on OPM.gov on the "How to Make a Payment" webpage.

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

Utilization of OLBP is voluntary. Should an OPM customer choose to make a payment via OLBP several steps must be taken by the OPM customer to submit a payment. Steps include: 1) Creation of online account with a financial institution, 2) Initiation of OLBP (or Bill Pay), 3) Setup/creation of a New Bill (to include a query for appropriate Payee, and keying-in of their OPM-designated Account Number, and Payee zip code), 4) Scheduling and submission of payment (to include payment amount and payment date for selected Bill).

OPM customers may use other payment methods to make a payment (e.g. check or money order). Note that a check payment provides OPM additional PII (e.g. Payer address and financial information, including financial account number).

If the OPM customer does not recognize the notification of payment due, the paper notification includes OPM contact information (phone number and address) for assistance. Additional information regarding payments to OPM is available on OPM.gov on the "How to Make a Payment" webpage.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that a customer may not recognize a notice of payment due or know how information is used or calculated within a system.

Mitigation: This risk is mitigated by providing customers with OPM contact information for assistance. In addition, this risk is mitigated through publication of this PIA.

Privacy Risk: There is a risk that a customer may not know how to make a payment to OPM utilizing online bill payment (OLBP) services.

Mitigation: This risk is mitigated by providing customers with step-by-step instructions on "How to Make a Payment" to OPM in both the notification letter and on OPM's public website (opm.gov).

Privacy Risk: There is a risk that a customer may not wish to utilize online bill payment (OLBP) services to submit payments to OPM.

Mitigation: This risk is mitigated by providing customers with a non-online, manual process for submitting a check or money order to OPM.

Section 5.0. Data Retention by the Project

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

The records are retained in accordance with the records retention schedules listed in Section 1.4. For business purposes, this generally means that records are retained for 7 years, although those records that become part of the retirement system records will be retained longer under the retirement records disposition schedule.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be retained for longer than necessary.

Mitigation: The risk is mitigated by defining and following an approved retention schedule and documented guidance from NARA.

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.

No. Generally the information collected in the OLBP project is not shared outside of OPM.

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

Not Applicable.

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

Not Applicable.

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

Not Applicable.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is no risk of information sharing.

Mitigation: Not Applicable.

Section 7.0. Redress

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

OPM customers may access their PPAI-OLBP relevant account information in two ways paper notifications received via the US Postal Service, and by contacting OPM directly. In addition, they may request access via the process outlined in the SORN identified in Section 1.2.

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

If the OPM customer does not recognize the notification of payment due or it contains incorrect information, they may contact OPM for assistance. In addition, should an OPM customer schedule an OLBP transaction, there is a defined timeframe (set by the financial institution and/or banking network) in which they can cancel or correct payment information. Individuals may also request amendment to their records by following the process outlined in the SORN identified in Section 1.2.

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

If the OPM customer does not recognize the notification of payment due or it contains incorrect information, the notification includes OPM contact information for assistance.

PPAI-OLBP does not change existing validation processes, and/or business rules. The non-OLBP (manual) payment transactions are validated, reconciled, and corrected, as needed. Processing of the OLBP transactions will be integrated into the existing processes. Should an error occur with applying an OLBP transaction, processes will be in place to investigate the payment in question (which may include contacting the Payer for validation).

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that customers may not understand how to access, correct, or amend their records maintained by OPM.

Mitigation: This risk is mitigated by providing customers with OPM contact information (via OPM paper notification letters and OPM's public website at opm.gov) should they require assistance or have questions regarding their OPM account or notification of payment due.

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?

PPAI-OLBP information and relevant systems are subject to OPM audit protocols, including inhouse audits. PPAI-OLBP ensures that only authorized parties have access to OLBP data. Authorized parties include individuals in OPM OCFO and OPM OCIO pertinent to the receipt, processing, and accounting of OLBP payments. OPM also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users are permitted access to the relevant systems or resources.

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

OPM federal staff and contractors are required to complete Security and Privacy Awareness training on an annual basis.

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

Only cleared OPM federal staff and contractors who are directly involved in the receipt, processing, and accounting of payments will have access to the OLBP data. OPM has authorities, duties, and processes defined which inform who has and/or receives access to such information.

OPM manages the authorization of access, to include both business operations (managed by OCFO) and technical operations and maintenance (O&M) (managed by OCIO). OCIO O&M acts at the discretion of OCFO regarding the processing of payments to OPM.

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?

Any agreements related to OLBP, or any new uses of or access to OLBP information, will be addressed by the Office of the Chief Information Officer and other relevant stakeholders within OPM, to include the Office of the Chief Information Officer and the Office of Privacy and Information Management, as appropriate.

Responsible Officials

Rochelle Bayard
Associate Chief Financial Officer

Approval Signatures

Signed Copy on file with Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer