



Privacy Impact Assessment (PIA) Template

JPP/Merit Central

(Name of the Information System or Information Collection)

October 2025

Date

System/Collection Overview

JPP/Merit Central (JPP/MC) is an existing, internally operated FHFA system that provides a platform for FHFA human resources personnel to deliver, develop, and update, as necessary, new compensation data, analyses, and/or employee salary increases and bonus reports. This system is composed of two separate components: JPP, which gathers data that is used to manage the process and produce a rating, which is also maintained in JPP, and Merit Central (MC), which pulls in final ratings of employees from JPP and is used to calculate bonus amounts for assigned employees. JPP/MC is also used to automatically calculate annual merit increases and performance-based bonuses based on the annual performance rating data contained in the system. JPP/MC likewise generates reports and transmits annual merit notification letters to employees.

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information types (e.g., contact information, demographic information, employment information) are being collected, used, disseminated, or maintained in the System/Collection?	JPP/MC contains the following personal information about FHFA employees: Name Social Security number (SSN) (MC Only) Position Title Grade Base Salary (MC Only) Before Merit and After Merit Pay (MC Only) Annual Performance Rating & Score Merit Increase dollars (MC Only) Total Merit increase dollars (MC Only) 75 th Percentile Range Maximum Lump-sum dollars (MC Only) Performance-Based Bonus (PBB) dollars (MC Only) Duty Station Location (MC Only) Employment Type (Full-time, Part-Time) (MC Only) Promotion Date (MC Only) Number of Months of Merit Increase Eligibility (MC Only)

1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	JPP obtains all PII from FHFA’s Active Directory except for an employee’s pay grade and position type (i.e., supervisor, non-supervisor, executive), which is provided directly by the employee. For MC, FHFA manually imports employees’ SSNs and current salaries from the Federal Personnel Payroll System (FPPS), which is owned and operated by the Department of Interior Business Center (IBC), FHFA’s shared-service provider for payroll services. MC also collects employees’ ratings from JPP.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	JPP/MC obtains information to 1) help facilitate the performance management process, including annual performance reviews, 2) calculate annual merit increases and performance-based bonuses, 3) produce related reports, and 4) transmit annual merit notification letters to employees.

#	Question	Response
1.4	How is the information provided to or otherwise obtained by the System/Collection?	For JPP, see section 1.2. For MC, FHFA personnel in the Office of Human Resources Management (OHRM) access FPPS and manually download the data to a spreadsheet, which is then provided to personnel in FHFA’s Office of the Chief Information Officer (OCIO) for upload to the MC system.
1.5	<p>Are Social Security Numbers (SSNs) being collected or used in the System/Collection?</p> <ul style="list-style-type: none"> • If yes, describe in detail: <ol style="list-style-type: none"> 1) The business justification for collecting or using SSNs; 2) The consequences if SSNs are not collected or used; and 3) How the SSNs will be protected while in use, in transit and in storage. <p>If no, state “N/A” in the response section.</p>	Yes, in MC only, SSNs are needed as a reference “bridge” to the IBC payroll system, which uses its own unique identifier. Without SSNs, the salary changes and PBB information could not be read by the IBC payroll system for automatic processing. To protect SSNs, they are maintained in a closed system, with access open only to authorized users for approximately 4-6 weeks per year, and reside behind an administrator’s firewall, where only authorized OHRM users have access. SSNs are also masked within the system.

Section 2.0 Uses of the Information

The following questions delineate the use of information.

#	Question	Response
2.1	How will the information be used and for what purpose?	JPP/MC is used for annual employee performance evaluations, annual merit increases, PBB decision-making and processing, and conducting salary-planning determinations.
2.2	Describe any types of measures or processes in place to ensure that information is only used in the manner for which it was collected.	Other than OHRM and OCIO employees with a business need-to-access MC, access to the MC portion of the system is only granted by the System Administrator and restricted to those employees who have a need for access and have been approved by the appropriate Division head or Office executive.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is the information retained?	For records subject to GRS 2.2, Item 040, which consist of official personnel actions, compensation and benefits, training and development, disciplinary and adverse actions, retirement or separation, and miscellaneous records such as grievances/complaints, collective bargaining agreements, and worker's compensation, these records are destroyed when survivor or retirement claims are adjudicated or when the records are 129 years old, whichever is sooner, but longer retention is authorized if required for business use. For records subject to GRS 2.2, Item 041, which consist of personal data, position and classification information, performance records, employment history, leave records, and other personal records such as emergency contact, employee data sheet, and citizen/immigration status, are destroyed when superseded or obsolete or upon separation or transfer of the employee, whichever is earlier.
3.2	Has a retention schedule been approved by FHFA's Records Management Office and National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (GRS) or FHFA specific Records Schedule number.	Yes, GRS 2.2, Item 040 for long-term temporary records and GRS 2.2, Item 041 for short-term temporary records.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and the individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	<p>Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification?</p> <ul style="list-style-type: none"> • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress. 	<p>Yes. This system is covered by FHFA-15, Payroll, Retirement, Time and Attendance and Leave Records; OPM/GOVT-1, General Personnel Records; and OPM/GOVT-2, Employee Performance File System Records.</p>
4.2	<p>How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? If notice is not provided, explain why not.</p>	<p>A Privacy Act Statement explaining that this information would be collected was provided to all employees at the time of hiring/onboarding via various onboarding forms. By way of example but not limitation, OPM Form SF181, which includes a Privacy Act statement and requires the disclosure of the employee's full name and SSN, is provided to new hires for completion.</p>
4.3	<p>Is an individual's response to the request for information voluntary or mandatory?</p>	<p>Voluntary</p>
4.4	<p>What are the consequences if an individual declines to provide the information?</p>	<p>If an individual declines to provide the information, they may not be hired. Once the information is inputted into the JPP/MC system, individuals do not have the opportunity to have that information deleted, as the agency owns the performance and compensation data specific to each employee.</p>
4.5	<p>What are the procedures that allow individuals to gain access to their information?</p>	<p>For FHFA-controlled records covered by FHFA-15, individuals may submit a Privacy Act request to FHFA's Privacy Act Officer pursuant to 12 CFR §1204.3(b). See https://www.fhfa.gov/about/privacy for more information.</p> <p>For OPM-controlled records covered by OPM/GOVT-1 and OPM/GOVT-2, individuals must follow the procedures outlined in those SORNs to access their information.</p>

#	Question	Response
4.6	What are the procedures for correcting inaccurate or erroneous information?	<p>For FHFA-controlled records covered by FHFA-15, individuals may submit a Privacy Act request to FHFA’s Privacy Act Officer pursuant to 12 CFR §1204.3(b). See https://www.fhfa.gov/about/privacy for more information.</p> <p>For OPM-controlled records covered by OPM/GOVT-1 and OPM/GOVT-2, individuals must follow the procedures outlined in those SORNs to access their information.</p>

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	<p>Is information shared with internal office(s) or division (s)?</p> <ul style="list-style-type: none"> • If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose. • If no, please state “N/A” in the response section. 	Information in the system is shared with the respective Division or Office executives, or their designee(s) to facilitate the processing of annual merit increases and PBBs and to conduct salary-planning determinations. Information is segregated within the system so that each Division or Office can only access employees’ information related to their respective Division or Office.
5.2	<p>Is information shared with external (outside FHFA) agencies, organizations, contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector.</p> <ul style="list-style-type: none"> • If yes, please identify the information shared, and for what purpose. <p>If no, skip to Section 6.</p>	As described in Section 1.4, new salary and PBB calculations for employees as well as their SSNs are downloaded from MC and uploaded to IBC’s FPPS to allow IBC to process the salary changes and PBB payments. However, FPPS already contains employee SSNs.
5.3	<p>Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection?</p> <ul style="list-style-type: none"> • If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1. <p>If no and/or a SORN a does not apply, identify the legal authority that permits the sharing outside FHFA.</p>	Yes, the sharing of PII with IBC and FHFA contractor personnel is covered by routine use (5) in FHFA-15. The sharing of information covered by OPM/GOVT-1 and OPM/GOVT-2 with contractor personnel is authorized under routine use jj in OPM/GOVT-1 and routine use p in OPM/GOVT-2.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	<p>Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein?</p> <ul style="list-style-type: none"> • If yes, how will they gain access to the System/Collection? • If no, how will the agency control access to and use of that information? • Are there procedures or criteria documented in writing? If so, please describe. 	<p>FHFA OIG personnel will not have access to this information system or the information therein. Contractor personnel supporting OHRM may be granted access to the system in accordance with the security protocols described herein.</p>
6.2	<p>Are there any conflicts of interest with respect to the System/Collection or information? If so, identify the conflicts of interest and describe how they are addressed.</p>	<p>No</p>
6.3	<p>Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.</p>	<p>All FHFA employees are required to undergo Security, Privacy, and Records and Information Management training as part of new employee onboarding training and annually thereafter. In addition, individuals whose work duties and responsibilities involve the regular collection, use, storage, access, or maintenance of PII receive role-based privacy training.</p>
6.4	<p>Describe the technical/administrative safeguards in place to protect the data.</p>	<p>Access is enforced through Active Directory security groups as well as application accounts. Users must be assigned to a specific security group to access the JPP/MC and must also be granted a specific role within the application. Role-based access control limits access to resources and permissions based upon the user's role. Further, sensitive PII is encrypted within the SQL database.</p>

Section 7.0 Risk

The following questions describe the risk to the information within the System or Collection.

#	Question	Response
7.1	<p>Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.</p>	<p>The risks include compromise, inadvertent disclosure, and/or loss of control, potentially exposing an individual's personal data to fraudulent activity, including identity theft. To mitigate this risk, FHFA implements technical and procedural controls described in this PIA, including Sections 1.5, 2.2, 6.3, and 6.4. Further, all data is collected from trusted sources, which consist of FHFA's Active Directory, the individual employee, and FPPS.</p>
7.2	<p>Discuss the risks associated with the length of time data is retained and how those risks are mitigated.</p>	<p>Given the significant retention period, there are increased risks to privacy. Risks include compromise, inadvertent disclosure, and/or loss of control, potentially exposing an individual's personal data to fraudulent activity, including identity theft. Risks are mitigated as described in Section 7.1.</p> <p>In addition, historical data is stored within FHFA's Information Security Management (ISM) system drive that can only be accessed by authorized users designated by the JPP/MCC system Administrators. Further, access to MC portion of the system is only granted when FHFA is processing merit increases and PBBs. Once that process is complete, access to the MC portion of the JP/MCC System is turned off so no users other than System Administrators can access it.</p>
7.3	<p>Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.</p>	<p>The privacy risks include compromise, inadvertent disclosure, and/or loss of control of the data. These are mitigated by transferring the data to IBC via a secure data tunnel. Likewise, IBC has implemented appropriate security protocols as a shared service payroll provider for Federal agencies.</p>