Privacy Impact Assessment (PIA) Template

Employment Matters Tracking (EMT)

(Name of the Information System or Information Collection)

October 2024

Date

Tasha L. Cooper
Senior Agency Official for Privacy
(202) 649-3091
Tasha.Cooper@FHFA.gov

System/Collection Owner(s)			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Janice Kullman	janice.kullman@fhfa.gov	OGC	202-649-3077
Sam Parker	samantha.parker@fhfa.gov	OGC	202-649-1159
Executive Sponsor			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**

System/Collection Overview

EMT, an existing FHFA information system, was conceived to track employment-related matters such as performance and disciplinary cases, Equal Employment Opportunity cases both at the agency stage and the Equal Employment Opportunity Commission (EEOC) stage, Merit System Protection Board (MSPB) cases, and those cases that proceed to Federal Courts. EMT also incorporates management investigations into harassment allegations, and a more fulsome treatment of mixed cases and appeals that go to both the EEOC and the MSPB and whistleblower cases at the Office of Special Counsel (OSC).

The system will track the dates of the deadlines of these matters so that OGC can keep track of them. It will also track similar cases, in the event of discovery requests for how the agency has treated like cases in the past, or for the agency's own use in determining penalties for discipline cases that are similar to current or future cases.

In addition to the PII identified below, this system will, in some instances, note whether an employee has received discipline and the specific type of discipline. The system will also maintain records of filed EEO cases and the protected bases for them, such as race or gender, but without identifying the race or gender of the person involved. Each case will have a link to a file on the FHFA's M drive, which is restricted to a small number of 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?	Employee name, case name and number, type of claim, deadlines associated with agency processing or defense of the claim, for disciplinary matters the type of misconduct and for both misconduct and performance actions the proposing and deciding official.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	The Office of Human Resources Management (OHRM) provides information on the initial conduct and performance actions. For MSPB , OSC, EEOC, or court cases the deadlines are provided by those agencies/courts.

1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The system will collect dates for various stages of these matters so that OGC can keep track of them. It will also track like cases in the event of discovery requests for how the agency has treated like cases in the past, or for the agency's own use in determining penalties for discipline cases that are similar to present or future cases. It is a case management tool.
1.4	How is the information provided to or otherwise obtained by the System/Collection?	In instances where Agency management has initiated a personnel action against an employee, the information comes from OHRM. As noted above, the deadlines come from the forum in which the case exists. Much of the information in EEOC and MSPB cases comes from the employees themselves when they fill out the claim complaint or appeal forms.
1.5	Are Social Security Numbers (SSNs) being collected or used in the System/Collection? • If yes, describe in detail: 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. • If no, state "N/A" in the response section.	N/A

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?	For the efficient management of cases for OGC and to help ensure OGC is aware of all upcoming deadlines.
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.	Access will be limited to four lawyers and two OHRM ER staff and the ER staff have access only to performance and discipline cases.

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?	Seven years after exhaustion of all appeals.

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 2.3.020-021, GRS 2.3.030-035, and GRS 2.3.040-041.

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	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • 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.	Yes. This information system is covered by the following SORNs: EEOC/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeals Records; MSPB/GOVT-1, Appeal and Case Records; and OPM/GOVT-3, Records of Adverse Actions.
4.2	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.	The EEOC, OSC, and MSPB have Privacy Act notices on their intake forms.
4.3	Is an individual's response to the request for information voluntary or mandatory?	Voluntary
4.4	What are the consequences if an individual declines to provide the information?	If the employee wants to pursue remedies in these fora they have to provide the information. If they do not wish to provide the information, they cannot pursue the case.
4.5	What are the procedures that allow individuals to gain access to their information?	In most cases, the information is originally submitted by the employee. In misconduct or performance cases, the due process rights set out in 5 U.S.C. chapters 43 and 75 and the accompanying regulations provide that the agency must provide all the relevant information and evidence to the employee as part of the process. In EEO cases, EEOC regulations at 29 CFR 1614.108 require the agency to provide the complainant with a copy of the investigative file.
4.6	What are the procedures for correcting inaccurate or erroneous information?	The users of the system will be able to manually alter any information that is incorrect. If an employee changes the nature of their claim, they do so through the forum in which they have brought their case.

Section 5.0 Sharing and Disclosure

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

#	Question	Response

5.1	Is information shared with internal office(s) or division (s)? • 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.	OGC will provide access to employee relations cases to employees from the OHRM Employee Relations branch so they can track due dates and run searches on similar cases when deciding on a penalty or preparing discovery responses.
5.2	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. • If yes, please identify the information shared, and for what purpose. • If no, skip to Section 6.	The information will not be shared with any external organization, with the exception of reports run in response to discovery requests. Those reports will be shared with opposing parties who request them and with the forum where the dispute lies.
5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1. • If no and/or a SORN a does not apply, identify the legal authority that permits the sharing outside FHFA.	Yes. The information will only be used in adjudicating the cases before the fora that collect the records. Applicable routine uses include: in EEOC/GOV-1, routine use f. (To disclose information to another federal agency, to a court, or to a party in litigation before a court in an administrative proceeding being conducted by a federal agency when the government is a party to the judicial or administrative proceeding); in MSPB/GOVT-1, routine use e. (To an appropriate Federal or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order where there is an indication of a violation or potential violation of civil or criminal law or regulation); and in OPM/GOVT-3, f. (To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding).

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response

6.1	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? • 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.	No. Access to EMT information is controlled through Active Directory security groups. Users, all six of whom are FHFA employees, are assigned to the security group to gain access to EMT information.
6.2	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.	No
6.3	Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.	We will provide initial training to those authorized to use the system, including an emphasis on the sensitivity of the information and that none of the information should be shared with anyone who does not have a business need to know, such as employees who are witnesses or involved in the settlement of a case. All FHFA employees receive annual training on privacy and cyber security. In addition, those who will have access to this system will also be required to take role-based privacy training.
6.4	Describe the technical/administrative safeguards in place to protect the data.	This information is stored on FHFA's internal production SQL Server, located behind our firewall. Access is limited to internal users only, and system access is controlled through Active Directory security groups.

Section 7.0 Risk

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

#	Question	Response
7.1	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.	Information on court cases and MSPB appeals are public. However, EEOC information is confidential. The risks of losing EEOC information would be the possible exposure of knowledge that a person had engaged in protected activity which potentially could make them subject to reprisal and the agency liable for such reprisal.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The risks are mitigated by limiting the number of people with access to the system and by marking cases closed so that the time begins to run on the records retention schedule and records will be timely destroyed.
7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	The information shared will be sanitized before sharing externally. For example, the type of case and penalty of several different cases will be shared, but the name of the employee involved will not. Only information relevant to the case, e.g., "white male over 40 no prior EEO activity," will be shared.