Privacy Impact Assessment Template

EMPLOYMENT MATTERS TRACKING SYSTEM (EMT)
(SYSTEM NAME)

JUNE 7, 2019
DATE

David A. Lee
Senior Agency Official for Privacy
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024
(202) 649-3803
Privacy@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how personally identifiable information (PII) is handled. A PIA ensures that the handling of PII conforms to applicable legal, regulatory and policy requirements, helps determine the risks and effects of collecting, maintaining and disseminating PII in an electronic system, and examines and evaluates protections and alternative processes for handling PII to mitigate potential privacy risks.

OVERVIEW SECTION

- Provide a thorough, complete, and clear overview of the System and give the reader the appropriate context to understand the responses. Some questions to consider include:
  - What is the purpose of the System?
  - What will be the primary uses of the System?
  - How will this support the Division's/Office's/Program's mission?
- This section fulfills the E-Government Act's requirement for an introduction to members of the public who may be reading the PIA. PIAs may be made publicly available unless a determination is made to not make the PIA available because publication would raise security concerns and/or reveal classified or sensitive information.

SECTION 1.0 CHARACTERIZATION OF THE INFORMATION

- Identify what PII is collected such as, home address; Social Security number; financial account number; home, mobile or facsimile telephone number; or personal e-mail address and the source of the information. A question to consider is where does the data originate? (e.g., FHFA, Office of Personnel Management, Regulated Entities, other Financial Institutions, or third parties). A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g., a bank, an internet service provider, or a private organization).
- Identify the risks associated with the information being collected and the how that could affect an individual's privacy if the information is lost or compromised.
- If the System collects Social Security numbers describe the business need for Social Security number and it will be protected.
- If the System collects information from 10 or more members of the public, ensure that FHFA has received prior approval from OMB to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act. If you are unsure of this last requirement, contact the Office of General Counsel for assistance.

SECTION 2.0 USES OF THE INFORMATION

- Identify the primary uses of the information and how the information supports FHFA's or the Office's/Division's/Program's mission.
- Identify the controls that are in place to ensure the information will be used for the manner for which it was collected. For example, access to the information will be restricted to a limited number of staff who use the data for their specific program use.

SECTION 3.0 RETENTION

- The retention periods for data/records that FHFA manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule. For the data being created/ maintained in the System, these records schedules

are the authoritative sources for this information. For assistance, contact FHFA's Records Management Office.

-

SECTION 4.0 NOTICE, ACCESS, REDRESS AND CORRECTION

- The Privacy Act requires that "each agency that maintains a System of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. 552a(e)(1).
- Data can be retrieved in a number of ways, but there is usually a personal identifier associated with a record. If the System retrieves information by an individual's name or other unique identifier (e.g. social security number) it is a Privacy Act System and will need a SORN published in the Federal Register. The System may already have a Privacy Act SORN. If you do not have a published SORN, or are unsure whether one exists, contact FHFA's Privacy Office.
- If a name or other unique identifier is not used to retrieve information, it is possible that the System is not a Privacy Act System. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may still be protected from disclosure under the Freedom of Information Act.
- The agency has developed and published an agency specific Privacy Act Rule in the Federal Register (12 CFR Part 1204) that explains how individuals can gain access to information about themselves and correct errors, if appropriate.
- Any employee who knowingly and willfully maintains a System of Records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5,000.

SECTION 5.0 SHARING AND DISCLOSURE

- If you do not know whether or not Systems share data, contact either the business owner of the data, or the IT specialist who knows what interfaces exist between the Systems/applications. As an example, if your System/application shares data with another System/application, ask yourself whether you have access to the data in the interfaced System/application. If so, then your answer is yes and an explanation is needed.
- Also consider "other" users who may not be obvious as those listed, such as GAO, or FHFA's Office of Inspector General. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act SORN under the "Routine Use" section when a Privacy Act SORN is required. The more comprehensive the list, the better it is.
- You must first review the SORN to determine whether any information that may come from an existing SORN allows that information to be exchanged and used for these new purposes or uses. There are restrictions on the use and disclosure of information that are set forth in a SORN.

SECTION 6.0 ACCESS AND SECURITY

- Access to data by a user (i.e. employee or contractor personnel) within FHFA is determined on a "need-to-know" basis. This means to authorized employees or contractor personnel who have a need for the information to perform their duties may be granted access to the information. Factors to consider in making this determination include the user's job requirements including supervisory responsibilities.
- The criteria, procedures, controls and responsibilities regarding access must be documented in order to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy.

- The System owner is responsible for ensuring that access to information and data is restricted to authorized personnel. Usually, a user is only given access to certain information that is needed to perform an official function. Care should be given to avoid "open Systems" where all information can be viewed by all users. System administrators may be afforded greater access – i.e. to all of the data – depending upon the System and/or application. However, restrict access when users do not need to have access to all the data.
- When a contract provides for the operation of a System on behalf of FHFA, the Privacy Act requirements must be applied to such a System. Contact the Contracting Officer or Contracting Officer's Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.
- The Security Assessment and Authorization (SA&A) process requires a System security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require monitoring of Systems to ensure that only authorized users can access the System for authorized reasons. In doing so, consider what controls are in place to ensure that only those authorized to monitor the System can in fact monitor use of the System. For example, business rules, internal instructions, and posting Privacy Warning Notices address access controls and violations for unauthorized monitoring. System Owners are responsible for ensuring that no unauthorized monitoring is occurring.
- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are System-based means by which the ability to access a System is either explicitly enabled or restricted. System Owners are responsible for ensuring that no unauthorized access is occurring.
- The IT Security Plan describes the practice of audit trails. An audit trail maintains a record of System activity and user activity including invalid logon attempts, access to data and monitoring. The SA&A process requires a System security plan outlining the implementation of the technical controls associated with identification and authentication.
- Every System/application/process that uses data must have controls in place to prevent the misuse of the data by those having access to the data. For instance, in computerized Systems, the Security Information Record (SIR) is part of the Core Storage Terminal Table. The SIR is the automated tool that identifies and authenticates an individual for the System and is transparent to the user.

PIA FORM

Overview

Provide an overview of the System and address the following:

- The System name and the division/office that owns the System;
- The purpose of the program, System, or technology and how it relates to the agency's mission; and
- A general description of the information in the System.

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Janice Kullman	Janice.kullman@fhfa.gov	OGC	202-649-3077
Gail Baum	Gail.baum@fhfa.gov	OGC	202-649-3061

System Overview:

EMT tracks employment–related matters such as performance and disciplinary cases, and Equal Employment Opportunity (EEO) cases both at the agency stage and the Equal Employment Opportunity Commission (EEOC) stage. It also covers Merit Systems Protection Board (MSPB) cases and those cases that proceed to Federal Courts. Later releases will also incorporate 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 collect dates for various stages of these matters so that OGC can keep track of the deadlines associated with 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 like cases.

In addition to the PII identified below, this system will, in some instances, note that an employee has received discipline and of what specific type, and that they have filed EEO cases and the protected bases for them, such as race or gender, but without identifying what race or gender the person identifies.

Each case will have a link to a file on the M drive which is restricted to a small number of employees. Initially access will be limited to 6 employees, but additional employees may be added if work load requires and there is a need to know.

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 program, System, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is being collected, used, disseminated, or maintained in the System?	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 in the System?	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 the deadlines associated with 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 like cases. It is a case management tool.
1.4	How is the information provided to FHFA?	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 complaint or appeal forms.
1.5	Given the amount and type of information collected, what are the risks to an individual's privacy that are associated with collection of the data? Explain in detail how the loss, or compromise of the information will/can affect an individual's privacy.	Information on court cases and MSPB appeals are public. However, EEOC information is confidential. The risks of losing EEOC information would be knowledge that a person had engaged in protected activity, which potentially could make them subject to reprisal and the agency liable for such reprisal.
1.6	Are Social Security numbers are being collected or used in the system?	No.

#	Question	Response
1.7	If SSNs are collected or used in the system, 1) describe in detail 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.	N/A

Section 2.0 Uses of the Information

The following questions delineate the use of information and the accuracy of the data being used.

#	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 controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	Access will be limited to 6 employees initially. Access will limited to a need to know basis, and any non-lawyers (i.e. employee relations staff) will only have access to performance and discipline cases maintained in the system.

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 NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	Yes. GRS 2.3.020-021, GRS 2.3.030-035, and GRS 2.3.040-041, and GRS 2.3.060-062.
3.3	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.

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 an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Has a System of Record Notice (SORN) been created? If so, provide the SORN name and number. If one has not, and one is required, provide the name of the SORN and the expected publication date in the Federal Register.	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	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	Yes, EEOC, OSC, and MSPB have privacy act notices on their intake forms.
4.3	Do individuals have the opportunity and/or right to decline to provide information? 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.
4.4	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.
4.5	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	With which internal organization(s) is the information shared? What information is shared and for what purpose?	OGC will provide access to employee relations cases to employees from the Office of Human Resources Management Employee Relations branch so they can track due dates and run

#	Question	Response
		searches on similar cases when deciding on a penalty or preparing discovery responses.
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	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 original information collection? If so, is it covered by an appropriate routine use in a SORN? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA.	Yes. The information will only be used in adjudicating the cases before the fora who collect the records.
5.4	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, so, 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."

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing?	The users will be restricted initially to 6 employees (two system owners, two attorneys, and two employee relations staff. Others may be added if work load requires access and there is a need to know. There are written procedures for users to request access.
6.2	Will non-FHFA personnel (e.g. contractor personnel, regulated entity personnel) have access to the System and information contained therein? If yes, how will they gain access to the System? How will the agency control their access and use of information? Are there procedures documented in writing?	No.
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the program or System?	We will provide initial in-person 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

#	Question	Response
		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.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Auditing will take place within Audit Central where users' actions, date, time and IP address will be recorded. Audit logs will be provided to the system owners, and will be reviewed at least monthly.
6.6	Has a Security Assessment & Authorization (SA&A) been completed for the System or Systems supporting the program? If so, provide the date the last SA&A was completed. If not, and one is required, provided the expected completion date of the SA&A.	No, however a SA&A will be completed upon completion of development.
6.7	Has an Authority to Operate (ATO) been issued for this System? If so, what date was it issued, and for how long was it issued? If not, when do you anticipate such ATO being issued?	No, it will be issued after development and testing is completed.