Privacy Impact Assessment Template

ENTELLITRAK
(SYSTEM NAME)

08/03/2021
DATE

Privacy Office
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 collected, stored, maintained, and shared. A PIA must be completed when FHFA: 1) develops or procures an IT System or project that collects, maintains, or disseminates PII from or about members of the public; or 2) initiates a new electronic collection of PII for 10 or more members of the public. System Owners are primarily responsible for completing the PIA with assistance from IT developers, IT security officers, and the Privacy Office.

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 if the System contains information about individuals, versus statistical, geographical, or financial information, with no link to a name or other identifier, such as, home address, social security number, account number, home, mobile or facsimile telephone number, or personal e-mail address.
- Examples of sources of the information include information that comes from an individual applying for a loan or mortgage, or other forms that an individual completes. A question to consider:
  - 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).
- 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 Privacy Act requires an agency to address the retention and disposal of information about individuals. This retention information is published in the Privacy Act System of Record Notice (SORN).

- 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.
- Disposing of the data at the end of the retention period is the last state of life-cycle management. Records subject to the Privacy Act have special disposal procedures (e.g. shredding of paper documents).

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.
- All employees, including contractors, have requirements for protecting information in Privacy Act Systems. Describe the controls in place, including any privacy and security awareness controls such as training materials, to protect the information.

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**
Brian Guy	**Brian.guy@fhfa.gov**	**OEOF**	**202-649-3019**

System Overview: Briefly describe the purpose of the program, System, or technology, and the information in the System, and how it relates to the agency's mission.

The Entellitrak Civil Rights application accelerator allows FHFA the tools to effectively create, track, maintain, and manage EEO cases to their successful completion. Entellitrak gives EEO caseworkers and managers the tools to guide, provide input, and report on all data elements and processes throughout the course of ongoing and closed civil rights cases. The system also allows the Agency to file legally required EEOC reports.

The database contains information regarding the names of individuals involved in an EEOC case and the factors (such as race, national origin, disability, etc) that are the basis of the case. It also contains intake forms, correspondence, investigative reports, settlement agreements, and case decisions. These documents may contain social security numbers, personal addresses and telephone numbers, and employment records including disciplinary files.

FHFA is also further required to prevent and address any discrimination in the agency. This software also allows the Agency to identify trends based on EEOC cases, which can assist the agency with addressing any issues related to discrimination.

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?	Individuals' Equal Employment Opportunity (EEO) complaints, settlements, medical records/diagnoses, personnel records, disciplinary records, names, addresses, phone numbers, date of birth information, Social Security numbers, age, race, national origin, sex, color, religion, genetic information. Alternative Dispute Resolution matters and harassment records may also be included.
1.2	What or who are the sources of the information in the System?	Agency officials, applicants for employment, OHRM records, employee testimony, medical professionals, current and former employees, EEO Counselors, EEO Specialists and Investigators; investigative report documents and witness and/or manager affidavits.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	Equal Employment Opportunity Commission (EEOC) complaint and hearing process; EEOC, DOJ, OPM, and Congress reporting requirements.
1.4	How is the information provided to FHFA?	Through document requests as part of investigations, witness interviews, EEO investigators, EEO counselors EEO Specialists, employees, and applicants. EEOC also provides documents.
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.	If files are accessed by inappropriate personnel or if EEO case information is obtained, sensitive data about Agency management decisions concerning disciplinary actions taken against the employee, employee performance information, and employee EEO activity may become available to those outside the EEO process. Such a breach would compromise the employee's privacy and confidentiality. We redact PII and sensitive data in complaint files to reduce the potential for identity theft. In most instances, case numbers are used in lieu of complaint names.

#	Question	Response
1.6	Are Social Security numbers are being collected or used in the system?	No.
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.	We do not collect Social Security numbers. However, sometimes older personnel records that are used in EEO cases may contain the Social Security numbers of employees or applicants. When this occurs, we redact the employee or applicant's social security number prior to placing the record in the system.

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?	The information is used by FHFA to litigate EEO cases, and also to provide required complaint data to the EEOC, DOJ, OPM, and Congress. We also use the data to resolve complaints, complete hearing records, respond to adhoc requests, and for training purposes.
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.	The software has security features in place. Only authorized users within OEOF have access to the system. We submit case information to the EEOC directly through their secure portal. When submitting the required reports, FHFA does redact case information is that is not needed for reports. Also, when using any information during any training scenarios, FHFA does not include PII or further relevant identifying details about a case.

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?	This will depend on the case. Once the case is resolved the record should be destroyed seven years after case resolution.
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. 5.3b Human Resource Record GRS 2.3, Item 111
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	If files are accessed by inappropriate personnel or if EEO case information is obtained, sensitive data about Agency management decisions, disciplinary actions and employee EEO activity may become available to those outside OEOF who do not need to know. We redact PII and sensitive data in complaint files. In most instances, case numbers are used in lieu of complaint names. Data is stored encrypted at rest and access to the system is password protected and limited only to authorized OEOF users.

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.	Yes. EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Records
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	Yes. Privacy Act Notice is provided to employees on intake forms and formal complaint forms.

#	Question	Response
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?	Yes. However, if the complainant fails to provide information it may impact the ability to process their complaint /or the dismissal of their complaint.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals who file complaints receive a copy of the Counselor's report and the Report of Investigation (ROI) as part of the EEO case process. Also, they may file a request under the Privacy Act using the procedures set forth in FHFA's Privacy Act regulation – 12 CFR 1204.
4.5	What are the procedures for correcting inaccurate or erroneous information?	The investigative reports are reviewed by the employee and they can request changes with the Agency. At the hearing stage the employee can request changes to the record with the Administrative Judge. Changes may also be made under the procedures set forth in FHFA's Privacy Act regulation – 12 CFR 1204.

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?	If a hearing is requested, OGC is provided with the ROI and complaint file in order to defend the Agency in EEO matters. OHRM is also provided with the name of the employee for data requests from OGC. Settlement agreements are shared with OHRM and OBFM for processing. The Agency Director is also made aware of the facts of high profile cases. Management officials and witness of various offices become aware of pending investigations and the alleged issues when their testimony is required for those cases.

#	Question	Response
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 EEOC is provided with complaint files and reports which include Agency demographics, case type, complaint issues, settlement/ADR and case processing times. Congress, DOJ, EEOC and OPM also receive reports with similar information as required by law. Federal courts may also receive the complaint file. OIG gains access to EEO information during audits and investigations. In instances of EEO claims/cases within FHFA's EEO office or the Agency Director (conflict cases), the FDIC /or CFPB is provided with the claim/complaint information to handle such claims on FHFA's behalf per Memorandum of Understandings (MOUs) we have with both agencies.
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, sharing this information outside of the agency is compatible with the original information collection. It is covered by the "EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Record" SORN. Both 29 CFR 1614 and EEOC Management Directive Agreement 110 permits the sharing of information outside of the agency for conflict matters as we, The contract investigator and/or counselor is authorized by the Agency to carry out is responsibilities under 29 CFR section 1614. Former employees and applicant witnesses may become aware of information under this CFR as well. We have existing MOUs with CFPB and FDIC to handle our conflict matters. These agreements are authorized by EEOC Management Directive 110.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	The risks to the individual include both: the loss of control of PII and the release of potentially sensitive data regarding the Agency decision/actions in response to EEO claims outside of the EEO process. Individual data is redacted to the extent possible when submitting required reports. Also, in addition to complying with the requirements of

#	Question	Response
		the Privacy Act, Complaint files are uploaded directly to the security EEOC portal. When FHFA disseminates any required investigation information externally, FHFA does so via the Agency's secure e- mail system, and the documents are password-protected.

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?	Only designated OEOF employees have access. The OEOF Director determines who is granted access and is designated as the responsibility of the customer agency within the Entellitrak FedRAMP package. Yes, the procedures are documented in writing, per OEOF's standard operating procedures.
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?	Yes, FHFA's OEOF contractors who have specifically been authorized by the iComplaints system owner will have access to the data. Permissions will be granted based on the concept of least privilege. OEOF staff are able to monitor what information the Contractors access in the system and whether information is removed or downloaded. Yes, the procedures are documented in writing, per OEOF's standard operating procedures.
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?	Entellitrak provides an online manual for system operations and has a webinar which may be accessed up system users upon request.

#	Question	Response
		Additionally, Entellitrak representatives may have access to the system in order to perform maintenance and troubleshoot technical issues.
6.4	Describe the technical/administrative safeguards in place to protect the data?	Entellitrak is included in the MicroPact Product Suite Federal Risk and Authorization Management Program (FedRAMP) authorization package. Further, FHFA will develop Customer Controls that describe the Agency's implementation of controls designated as the responsibility of the customer agency within the Entellitrak FedRAMP package. This includes procedures for securely managing access to the system, assigning roles based on the concept of least privilege, reviewing audit logs, etc.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Entellitrak captures logs of all user actions on the system, and at least monthly, the system owner will review events from the last 30 days and notify IT Security when the logs have beenreviewed, noting if any unusual activity was observed.
6.6	Has a 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.	Entellitrak is included in the MicroPact Product Suite which received its initial FedRAMP Authorization on June 6th, 2014. I t is in the continuous monitoring phase of the FedRAMP program and FHFA reviews the status of ongoing assessments at least annually.
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?	FHFA will issue an Agency ATO for Entellitrak within 60 days of acquiring the solution.