Privacy Impact Assessment Template

ENTELLITRAK ANTI-HARASSMENT TRACKING SYSTEM
SYSTEM NAME

November 2022
DATE

Tasha L. Cooper
Senior Agency Official for Privacy
(202) 649-3091
Tasha.Cooper@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 Information Technology (IT) system or project that collects, maintains, or disseminates PII that can be used to identify a specific individual; or 2) initiates a new electronic collection of PII for 10 or more members of the public, which includes any information in an identifiable form permitting the physical or online contacting of a specific individual.

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 or Mobile Phone Number**
Kendrick T. Gibbs	Kendrick.Gibbs@fhfa.gov	Office of Equal Opportunity and Fairness (OEOF)	202-360-0161

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 Anti-Harassment Tracking System provides FHFA the tools to effectively create, track, maintain, and manage harassment cases to their successful completion. Entellitrak gives harassment caseworkers and managers the tools to guide, provide input, and report on all data elements and processes throughout the course of ongoing and closed harassment concerns.

The system contains information regarding the names of individuals involved in both equal employment opportunity (EEO) concerns (e.g., race, national origin, disability) and non-EEO harassment concerns that are the basis of the case. It also contains intake forms, correspondence, inquiry reports, and case decisions.

FHFA is required to address and prevent harassment in the Agency. This system provides the Agency with tools necessary to identify trends based on Equal Employment Opportunity Commission (EEOC) cases, which can assist the Agency with addressing issues related to harassment.

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?	The harassment concerns of individuals and documents associated with such concerns may include medical records, personnel records, personal and business contact information, demographic information, and genetic information.
1.2	What or who are the sources of the information in the System?	Agency officials, applicants for employment, Office of Human Resources Management (OHRM) records, employee testimony, current and former employees, EEO Specialists, contract Investigators; investigative report documents, witness and/or manager affidavits, and members of the public.

#	Question	Response
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	To fulfill the requirements of FHFA harassment process and comply with applicable law, as well as to report as required to the EEOC, U.S. Department of Justice (DOJ), U.S. Office of Personnel Management (OPM), and Congress.

1.4	How is the information provided to FHFA?	Individuals making a harassment claim to the FHFA voluntarily submit information and potentially records via the dedicated Anti-Harassment email address to support their claim. Thereafter, FHFA may obtain additional information from the complaining individual and/or potential witnesses in the course of investigating the claim via document requests, witness interviews, contract investigators, EEO Specialists, employees, and applicants.
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 harassment case information is obtained, sensitive data about Agency management decisions concerning disciplinary actions taken against the employee or manager, employee performance information, and employee harassment activity may become available to those outside the harassment process. Such a breach would compromise the employee's privacy and confidentiality and potentially cause that person embarrassment or subject them to blackmail or identity theft.
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.

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 collect and maintain harassment case information, to comply with EEOC regulations mandating a system of record for harassment complaints, and to fulfill requirements to report to the EEOC, DOJ, OPM, and Congress. FHFA may also use the data for ad hoc requests to gather data needed for required reporting and for training purposes; however, in all such instances all personal identifiers are removed from the data provided prior to any external reporting or internal use.

#	Question	Response
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.	Data is stored with encryption. Access to the system is password protected and limited to authorized OEOF users. Individuals who submit harassment complaints, after registering and creating a username and password to access the system can then gain access to their own complaint and related information, but not to any other complaint or harassment information. Also, when using any information during any training scenarios, FHFA does not include PII or any other 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?	Once the case is resolved, the physical record should be destroyed seven years after case resolution. However, we would keep data in our electronic system for reporting trends analysis information, as required by law.
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 harassment 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. Data is stored and encrypted. 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. A Privacy Act Statement is provided to employees on 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?	Yes. However, if the complainant fails to provide information it may impact the ability to process their harassment concern.

#	Question	Response
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals who file harassment concerns receive a copy of their witness statement. They are not provided a copy of the Harassment Inquiry Report (HIR) as part of the harassment case process. 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 harassment reports are reviewed by the OEOF staff for accuracy and sufficiency. 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?	After the HIR is completed, it is provided to the Office of General Counsel (OGC) and OHRM along with an assessment memo to provide corrective actions, if warranted. The Agency Director is made aware of certain cases as determined necessary.
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.	In addition to the routine uses identified in the applicable SORN for this system, the EEOC is provided with the HIR when a concurrent EEO complaint is filed, and a document request is made. Federal courts may also receive the complaint file. OIG gains access to EEO information during audits and investigations. Former employees and applicant witnesses may become aware of information under this CFR as well, for example,

		where such persons have information relevant to the investigation of a harassment claim.
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 government-wide SORN issued by the EEOC, EEOC/GOVT-1, which gives notice of routine uses of this information, provides that information in this system may be used: a. To disclose pertinent information to the appropriate federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation. b. To disclose information to another federal agency, to a court, or to 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. c. To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual. d. To disclose to an authorized appeal grievance examiner, formal complaints examiner, administrative judge, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee. e. To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding. f. To disclose information to officials of state or local bar associations or disciplinary boards or committees when they are investigating complaints against attorneys in connection with their representation of a party before EEOC. g. To disclose to a Federal agency in the executive, legislative, or judicial branch of government, in response to its request for information in

		connection with the hiring of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's decision. h. To disclose information to employees of contractors engaged by an agency to carry out the agency's responsibilities under 29 CFR part 1614. i. To disclose information to potential witnesses as appropriate and necessary to perform the agency's functions under 29 CFR part 1614. Both 29 CFR 1614 and EEOC Management Directive 110 permits the sharing of information outside of the agency for conflict matters. The contract investigator is authorized by the Agency to carry out is responsibilities under 29 CFR section 1614.
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 the loss of control of PII and the release of potentially sensitive data regarding the Agency decision/actions in response to harassment concerns. 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 has assigned an FHFA system owner who approves access to the system. The procedures are documented in the applicable Customer Controls per agreement with the vendor.
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, the vendor of the system has access to the system for routine maintenance/updates. As documented in the Customer Controls, the vendor will notify the FHFA system owner prior to accessing FHFA's system, and vendor personnel will do so only using named accounts that identify the individual accessing FHFA's system.

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 by system users upon request. All FHFA employees are required to undergo security, privacy, and Records and Information Management (RIM) training for use of FHFA systems at onboarding and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training, and role-based privacy awareness training for those individuals whose work duties and responsibilities involve the collection, use, storage, access, or maintenance of PII.
6.4	Describe the technical/administrative safeguards in place to protect the data?	Entellitrak is included in the Tyler Technology Product Suite Federal Risk and Authorization Management Program (FedRAMP) authorization package. Further, FHFA has developed 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, 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 quarterly the system owner will generate an audit log report, review system events, and notify IT Security when the logs have been reviewed, 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. It 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 anticipates issuing an Agency ATO for the Entellitrak Anti-Harassment system in November 2022.