Privacy Impact Assessment (PIA)

ENTELLITRAK ANTI-HARASSMENT TRACKING SYSTEM
(Name of the Information System or Information Collection)

November 2025
Date

System/Collection Overview
The Entellitrak Anti-Harassment Tracking System is an existing, contractor-operated, cloud-based system-as-a-service that provides FHFA the tools to effectively create, track, maintain, and manage harassment cases to their successful completion. Entellitrak gives harassment case workers 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. 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 System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of personally identifiable information (PII), such as name, address, social security number, date of birth, and financial information.

#	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?	The system maintains information related to harassment concerns of individuals and documents associated with such concerns. The types of records in the system may include medical records, performance records, personnel records, intake forms, correspondence, inquiry reports, and case decisions. The types of PII in the system may include personal and business contact information, medical information, demographic information (e.g., race, national origin, disability), and genetic information. Information may also include additional PII contained in a personnel record (e.g., Standard Form 50, Notification of Personnel Action) that is submitted with a complaint or gathered as part of an investigation. Such information may include, but is not limited to, position title, grade level, salary and other compensation information, personnel action taken, and the effective date of such actions.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	Agency employees and contractors, applicants for employment, Office of Human Resources Management (OHRM) records, EEO specialists,

		contract investigators, investigative report documents, witness and/or manager affidavits, and members of the public.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	To support FHFA's harassment complaint process, ensure compliance with applicable laws, and fulfill mandatory reporting requirements 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 or otherwise obtained by the System/Collection?	Individuals reporting a harassment claim to FHFA submit information and potentially records to the dedicated Anti-Harassment email address to support the claim. Thereafter, FHFA may obtain additional information from the complainant and/or potential witnesses while investigating the claim via document requests and interviews.
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.	Although SSNs are not requested or required to be submitted, individuals may submit personnel records in support of their harassment claim that contain their SSN. FHFA requires a complete and accurate factual record to assess harassment complaints and therefore does not restrict individuals from submitting documentation containing their SSN if the individual chooses to provide such information. Any such information is protected as described herein, including restricting access to the system, limiting dissemination of information contained in the system, and encrypting information stored in 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?	The information is used by FHFA to track and respond to harassment complaints as well as to comply with EEOC regulations mandating a system of records for harassment complaints, and to fulfill requirements to report to the EEOC, DOJ, OPM, and Congress. FHFA may also use the information for ad hoc requests to gather information needed for required reporting and for training purposes; however, in all such instances, all personal identifiers are removed from the information provided prior to any external reporting or internal use.

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.	Stored information is encrypted. Access to the system is password protected and limited to authorized 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.

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 a case is resolved, the record should be destroyed seven years after case resolution. However, information may be retained for longer periods for business purposes, including reporting trends analyses, as required by law.
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, Item 050, Harassment Complaint Case Files.

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. EEOC/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeal Records and OPM/GOVT-1, General Personnel Records.
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.	Yes. A Privacy Act Statement describing FHFA's purpose for collecting the information is provided on intake forms used to collect the information.
4.3	Is an individual's response to the request for information voluntary or mandatory?	FHFA managers, supervisors, and executives are required to report allegations of harassment they have observed, been informed of, or been alleged to have committed. Reporting is voluntary for all other individuals.

4.4	What are the consequences if an individual declines to provide the information?	FHFA managers, supervisors, and executives may be subject to disciplinary action if they fail to report harassment as required by FHFA policy. For other individuals, the failure to provide information may impact FHFA's ability to process their harassment concern.
4.5	What are the procedures that allow individuals to gain access to their information?	Individuals who file harassment concerns receive a copy of their inquiry statement. They are not provided with a copy of the Harassment Inquiry Report (HIR) as part of the harassment case process. Individuals may also submit a Privacy Act request for access to their information to FHFA's Privacy Act Officer pursuant to 12 CFR § 1204.3(b). Additional information regarding Privacy Act requests is available on FHFA's website Privacy page, located at https://www.fhfa.gov/about/privacy.
4.6	What are the procedures for correcting inaccurate or erroneous information?	Individuals may submit a request to amend or correct records to FHFA's Privacy Act Officer pursuant to 12 CFR § 1204.3(d). Additional information regarding the amendment of records pursuant to the Privacy Act is available on FHFA's website Privacy page, located at https://www.fhfa.gov/about/privacy.

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.	Yes. After the HIR is completed, it is provided to the designated Appropriate Management Official (AMO) with a copy to OGC and OHRM as consulting offices. The AMO is provided the information to review the case, determine whether harassment occurred in violation of the Agency's Anti-Harassment policy, and take corrective actions, if warranted. The Agency Director is made aware of certain cases as deemed necessary.
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 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 if relevant to a claim filed in federal court. FHFA OIG may be provided information from the system in response to audits and investigations. Individuals external to the Agency who are interviewed as part of an investigation may also be made aware of a

		limited amount of information from the system as part of the investigatory process.
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 does not apply, identify the legal authority that permits the sharing outside FHFA.	Yes, sharing this information outside of the agency is compatible with the purpose of the original information collection. It is covered by routine uses a, b, d, e, h, and i in EEOC/GOVT-1.

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.	Yes, the vendor for the system has access to the system for routine maintenance/updates. As provided in the customer controls documentation, the vendor will notify the FHFA system owner prior to accessing FHFA's system, and vendor personnel will do so using only named accounts that identify the individual accessing FHFA's system.
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.	Entellitrak provides an online manual for system operations and has a webinar which may be accessed by system users upon request. Additionally, all FHFA employees are required to undergo Security, Privacy, and Records and Information Management training for use of FHFA systems during onboarding and annually thereafter. All FHFA users with elevated privileges also receive specialized security training and role-based privacy awareness

		training for those individuals whose work duties and responsibilities regularly 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. It is in the continuous monitoring phase of the FedRAMP program. Further, FHFA has developed customer controls that describe the Agency's implementation of controls that are the responsibility of FHFA as the Customer Agency, and not the responsibility of the vendor. This includes the implementation of single sign-on authentication, procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, and generating and reviewing audit logs.

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.	If information from the system is improperly accessed or disclosed, sensitive PII and information about Agency management decisions, employee performance information, and employee harassment activity may become available to those outside the harassment process. The risks to an individual's privacy if the information is lost or compromised include identity theft, blackmail, embarrassment, and/or misuse of the individual's personal information. To mitigate these risks, access to Entellitrak and the information therein is limited to those who have a need-to-know in the performance of their official duties. Further, information is protected as described in Sections 2.2 and 6.4.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	There are risks associated with the retention of information given the lengthy retention period, which increases the risk of information being subject to a breach. While records may be destroyed seven years after a case is resolved, information from the records is kept for longer periods of time for business purposes including reporting and analysis. Risks of a breach are mitigated as described in Sections 2.2 and 6.4.

7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	There are risks associated with the external sharing of information, including accidental disclosure to the incorrect party and further disclosure by third parties. The risks to the individual because of external sharing include the loss of control of PII and the release of potentially sensitive information regarding Agency decisions/actions in response to harassment concerns. To mitigate these risks, FHFA shares only that information which is required and does so via the Agency's secure e-mail system, with documents being password-protected. System users also receive role-based privacy training to reduce the risk of inadvertent disclosure. Third parties that receive PII or other types of Controlled Unclassified Information (CUI) are notified of the information's protected status via CUI document markings or other means.