Privacy Impact Assessment Template

APPLICANT TRACKING SYSTEM
(SYSTEM NAME)

12/09/2016
DATE

This template is used when the Chief Privacy Officer determines that an IT System contains Personally Identifiable Information and a more in-depth assessment is required.

Complete and sign this template and forward to the Chief Privacy Officer.

David A. Lee
Chief Privacy Officer
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 information in identifiable form ("IIF"; also referred to Personally Identifiable Information (PII)) is handled. PIAs are to be completed when FHFA: 1) develops or procures an IT System or project that collects, maintains, or disseminates IIF from or about members of the public; or 2) initiates a new electronic collection of IIF for 10 or more members of the public. PIAs are not required for collections of information from Federal employees. IIF about government personnel generally is protected by the Privacy Act; however, the Office of Management and Budget (OMB) encourages agencies to conduct PIAs on these Systems, as appropriate. System Owners and Developers are responsible for completing the PIA.

The guidance below has been provided to help System Owners and Developers complete a PIA.

Overview

- In this section, provide a thorough 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 for 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.

FOR A PIA COMPLETE ALL SECTIONS.

FOR A MODIFIED PIA COMPLETE THE FOLLOWING SECTIONS ONLY:

- **Overview**
- **Sections 1, 2, and 6**

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 may 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 the Chief Privacy Officer.
- 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 the General Counsel Accountability Office or the FHFA 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 access 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.
- According to OMB Circulars A-123 and A-130, 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. Describe these processes in response to this question.
- 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

This section provides an overview of the System and addresses 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.

Date submitted for review: December 10, 2016

System Name: Applicant Tracking System			
System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Moji Adelekan	Moji.adelekan@fhfa.gov	OHRM	2026493745
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 Applicant Tracking System will be used by OHRM staff to post and publicize mission critical occupation job openings, and for receiving, storing, processing and tracking resumes and applications. The system is a Software as a Service (Saas) hosted externally to FHFA's site. The service provider is Acendre.			

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 collected, used, disseminated, or maintained in the System?	Name; date of birth; race;, national origin; color; home and business address; personal and business telephone numbers and email addresses; military status; education records; and employment status and/or records.
1.2	What are the sources of the information in the System?	Individuals responding to job postings or other events where FHFA is requesting resumes or contact information.

#	Question	Response
1.3	Why is the information being collected, used, disseminated, or maintained?	To support staffing function by collecting resumes of passive and active applicants for FHFA Mission Critical Occupations (MCO) positions and to build a bank of potential candidates for current and future job openings. Information collected may also be used for analysis of Race and National Origin data.
1.4	How is the information collected?	Directly from individuals who are interested in FHFA current or future job openings/positions.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	The risk to an individual's privacy if the data is lost or compromised is identify theft, loss of future employment opportunities, embarrassment, and/or misuse of the individual's personal information.

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	Describe the uses of information.	The system will be used for receiving, storing, processing and tracking applicant resumes.
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 employees that are only permitted to perform recruitment and staffing functions. Also, the system requires each individual to have a unique username and password, and they are required to agree to the terms of the privacy statement before accessing the system. The System Administrator will monitor ATS for appropriate use.

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 information retained?	7 years
3.2	Has a retention schedule been approved by FHFA's Records Management Officer and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	Yes, records will be managed in accordance with FHFA's *Comprehensive Records Schedule* (CRS), Item 6.1.b – Projects with department-wide or administrative impact.

#	Question	Response
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	OHRM will work with Records and Information Management (RIM) to document and approve disposition activity on applications that are 7 years old.

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. Applicant Tracking System – FHFA - 25. The expected publication date is by the end of the calendar year 2016.
4.2	Was notice provided to the individual prior to collection of information?	Yes
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes – Applicant's submission of their resume/curriculum vitae is voluntary.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals who submit a resume through the system can log in via a unique username and password created by the individual. Through unique user names and passwords, applicants can access their individual accounts. They will be able to view the information they have uploaded and the status of their applications.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Correction will be applicant and FHFA employee driven.

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?	Information is shared with hiring managers. Resume will be shared but not race, national origin, gender, or ethnicity.

#	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.	Information typically will not be shared with external organizations, except for analysis of race, national origin or gender of the applicants/hires, or for ligation purposes. External organizations include GAO, EEOC, OPM, MSPB, Congress and other administrative or judicial tribunals.
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. Yes.
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	The risk to an individual's privacy if the data is lost or compromised is identify theft, loss of future employment opportunities, embarrassment, or misuse of the individual's personal information. These risks are mitigated by only sharing aggregate data; or only that PII which is necessary to be shared.

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? If so, attach a copy to this PIA.	Standard Operating Procedure will be drafted once roles and responsibilities have been identified in ATS.
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? If so, attach a copy to this PIA.	Yes. Authorized Acendre (Service provider) will have access to the system. Users and administrators will gain access by unique ID and password. Access will be controlled by assigned roles. The System Administrator will determine what activities/functions each user will need. Based on that determination, the user will be assigned a role that only allows access to authorized functions. The System Administrator will review these roles and access on an annual basis.

#	Question	Response
6.3	Describe the training that is provided to users either generally or specifically that is relevant to the program or System?	No Training has been provided yet. Training will be provided to all users before using the system.
6.4	What technical safeguards are in place to protect the data?	The connection to the application is encrypted using Secure Hash Algorithm (SHA) 256. Acendre protects confidentiality and integrity of sensitive PII by implementing Amazon Web Services (AWS) Key Management Service (KMS) and Elastic Block Storage (EBS) Simple Storage Service (S3) data-at-rest encryption.
6.5	What auditing measures are in place to protect the data?	The application includes a Configuration Log which allows the system owner to view the date a change was created, the user that created the change, the actions taken by the specific user, a description of the action taken, and the job name that was created/modified/deleted. Each item logged in the Configuration Log has a ID unique to the user that created the change.
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.	The Security Assement Report (SAR) was completed on ~~Yes~~ – September 30, 2016. The authorization to operate (ATO) meeting is being scheduled. Ralph Mosios

Signatures

Moji Adelekan
System Owner (Printed Name) — MAdelekan
System Owner (Signature) — 12/08/16
Date

N/A
System Developer (Printed Name) — System Developer (Signature) — Date

Ralph Mosios
Chief Information Security Officer (Printed Name) — Ralph Mosios
Chief Information Security Officer (Signature) — 12/15/2016
Date

Kevin Winkler
Chief Information Officer (Printed Name) — Chief Information Officer (Signature) — 12/15/16
Date

David A. Lee
Senior Agency Official for Privacy (Printed Name) — Senior Agency Official for Privacy (Signature) — 12/19/2016
Date