Privacy Impact Assessment Template

FHFA GENERAL SUPPORT SYSTEM
(SYSTEM NAME)

MAY 14, 2019
DATE

This template is used when the Senior Agency Official for Privacy 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 Senior Agency Official for Privacy.

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

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how Personally Identifiable Information (PII) is 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.

Below is guidance, by section, for a System Owner to follow when completing a PIA.

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.

FOR A FULL PIA

- **COMPLETE ALL SECTIONS**

FOR A MODIFIED PIA - Under certain circumstances the Senior Agency Official for Privacy may make a determination that a complete PIA is not necessary depending upon the nature and extent of the PII collected. When the SAOP makes such a determination, the System Owner only needs to complete the following sections of the PIA template:

- **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 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

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: May 14, 2019

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Tom Leach	Thomas.leach@fhfa.gov	OTIM	202-649-3640

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 FHFA GSS is fault-tolerant system providing best-of-breed technology in support of the FHFA mission. The FHFA GSS, due to its geographically-dispersed topology, is considered a WAN (Wide Area Network) and consists of the backbone, a Metropolitan Area Network, and the LANs at the various sites. The GSS provides connectivity between the Agency's sites, Headquarters, and Data Centers; Internet access, Voice over IP (VOIP) telephone services, e-Mail and directory services for all Agency divisions and offices. The FHFA GSS provides information sharing and data processing capabilities via interconnected workstations and servers. The Agency employs a variety of applications supported by or dependent on access to the GSS. The GSS includes a segregated Extranet that allows regulated entities such as Freddie Mac, Fannie Mae and the FHLB Banks to submit data to FHFA. The GSS is extended for mobile users with Apple iPhones and 802.11i Wi-Fi Protected Access (WPA) Points using Advanced Encryption Standards (AES) Encryption at Constitution Center, Freddie Mac and Freddie Mae and the FHLBank sites. Secure network access to Agency resources are provided through encrypted Virtual Private Network (VPN) connections across public networks. Remote access is available via an always-on Microsoft VPN and GlobalProtect. FHFA supports a Citrix Virtual Desktop Infrastructure (VDI) solution that provides access to local information resources using a web browser in conjunction with a Citrix client. The Citrix solution provides authentication using a two-factor authentication schema.

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?	Much of the information processed on or transmitted through the FHFA GSS relates to network users and their basic Active Directory account information, e.g., FHFA usernames, contact information, audit logs, etc. However, a number of FHFA applications reside on the FHFA GSS, including mission focused applications, and internal administrative applications. These applications have separate PIAs that are available on the FHFA.Gov website. Information specific to the FHFA GSS includes, but is not limited to the following: - Employee or Contractor name; - FHFA Username; - Business Email address; - Duty station location; - Business telephone numbers; - Internet Protocol (IP) address; - Network audit history (login, logout times, internet usage logs); - Password (stored as a hash value); - PIN (stored as a hash value).
1.2	What or who are the sources of the information in the System?	The information contained in the FHFA GSS is primarily derived from current and former FHFA network users, including current and former employees, interns, and contractors; and FHFA hardware, software and system components that generate information reflecting activity on the FHFA network.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The information is collected, used, disseminated and maintained to enable effective, reliable and secure operation of the FHFA network in support of FHFA's business offices and mission. The information collected is required to create and maintain secure network accounts for FHFA employees, contractors and extranet users, and to allow these users to utilize FHFA network

#	Question	Response
		resources such as email, word processing, instant messaging, voice over internet protocol (VOIP), etc.
1.4	How is the information provided to FHFA?	The information processed by the FHFA GSS is partially collected from communication with users as part of the on-boarding processes that includes identity verification and fingerprinting as part of background investigation adjudication. Active FHFA network users can generate additional information that is reflective of their network activity that includes information such as: security logs of access to applications, Internet use, VOIP call logs, Skype communication, etc. The GSS also receives information that includes information from external entities, e.g., the Dept. of Interior (DOI) as part of the Human Resources Information System (HRIS), Office of Personnel Management (OPM) eDelivery system, etc., receiving this information via site-to-site virtual private network (VPN) connections, or Connect:Direct connections. These additional sources of information have separate PIAs.
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.	There is minimal impact associated with the loss or compromise of the information maintained in the GSS. The information elements, including name, duty station location, work telephone numbers and work account name are not normally publicly available, but do not pose a higher risk of subsequent identity theft or personal harm to the individual if released.
1.6	If Social Security numbers are being collected, provide the legal authority for the collection. In addition, describe in detail the business justification for collecting SSNs, what the consequences would be if SSNs were not collected, and how the SSNs will be protected while in use, in transit and in storage.	N/A. SSNs are not collected and stored specifically by the GSS. Rather, they are collected and stored in specific applications which have separate PIAs and System of Records Notices, as required.

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 collected is required to create and maintain secure network accounts for FHFA employees, contractors and extranet users, and to allow these users to utilize FHFA network resources such as email, word processing, instant messaging, voice over internet protocol (VOIP), etc.
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 to FHFA GSS information systems is managed through Active Directory security groups to ensure that users are granted access based on group membership to only those network resources for which the user has a legitimate business need.

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?	FHFA uses Veritas' Enterprise Vault (Evault) for the management of permanent and temporary electronic records in accordance with FHFA's *Comprehensive Records Schedule* (CRS). Records and Information Management (RIM) assigns a retention to each user's archive based on their Office and the role they play in the Agency. Network and security audit records are maintained within FHFA's Security Information and Event Management (SIEM) solution for one year.
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.	Records are managed in accordance with FHFA's CRS and based on the retention assigned to each user's archive based on their Office and the role they play in the agency. Records pertaining to the management of Evault system will be managed in accordance with FHFA's CRS Item 5.4 – Information Technology and Management Records.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Risk: Disposition (reviews, approvals, and deletions) may not be carried out as required in the normal course of business due to external circumstances such as litigation holds.

#	Question	Response
		Mitigation: Instituted annual reviews of disabled accounts to update status as necessary.

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.	No. A SORN is not required.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	N/A
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?	N/A
4.4	What are the procedures that allow individuals to gain access to their information?	N/A
4.5	What are the procedures for correcting inaccurate or erroneous information?	N/A

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?	FHFA's Office of Technology and Information Management (OTIM) manages FHFA GSS information. Access to the data is limited to those with an operational need to access the information, such as IT administrators and engineers.

#	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.	FHFA's GSS information extends to the Microsoft Azure cloud environment, which is utilized as part of FHFA's Exchange Online Protection (EOP) implementation. This is captured in the Microsoft Azure Active Directory Sync PIA. Microsoft Azure is considered within the authorization boundary of the FHFA GSS. FHFA utilizes Federal Shared Service providers to provide government-wide services such as background investigations, HSPD-12 management, payroll, travel services, financial management, etc. These systems are covered by PIAs completed by the providing 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.	N/A. The sharing of FHFA information outside of the agency is covered by separate PIAs and SORNs and does not apply to the FHFA GSS.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	All federal shared service providers are subject to the Federal Information Security Modernization Act of 2014 (FISMA) and the Privacy Act.

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, provide a signed copy to the Privacy Office.**	The FHFA GSS System Security Plan describes how the GSS meets all NIST SP 800-53 Revision 4 security controls including AC-2, Account Management.
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, provide a copy to the Privacy Office.**	Help Desk staff and IT engineers with access to GSS information may consist of FHFA employees and contractor personnel. All users undergo personnel screening prior to gaining access to FHFA's network and are required to complete security and privacy awareness training within two weeks of their start date. Active Directory groups are used to apply permissions to all users based on the concept of least privilege. The Account Management Standard Operating Procedures (SOP) describes the

#	Question	Response
		procedures for using AD groups to restrict access to information based on a user's business need.
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?	FHFA has mandatory annual IT Security and Privacy Awareness training as well as Records Management training along with specialized security training requirements for users with elevated privileges.
6.4	Describe the technical/administrative safeguards in place to protect the data?	The FHFA GSS SSP describes the controls in place to protect the confidentiality, integrity and availability of data maintained within the GSS and transmitted across the network, that includes, but is not limited to: - Multi-factor authentication for all privileged and non-privileged users; - Hard disk encryption on all FHFA workstations; - Layer-7 Intrusion Prevention System (IPS) and web-proxy; - Secure email filtering; - Einstein 3A protections; - Always-on encrypted Virtual Private Network (VPN);
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Active Directory group policy changes are audited by Active Administrator and provided to IT engineers and IT security personnel for in real-time.
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 GSS is in the continuous monitoring phase of the Risk Management Framework and undergoes annual security control assessments. The last SA&A was completed on September 11, 2018.
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? **Provide a copy to the Privacy Office.** If not, when do you anticipate such ATO being issued?	The most recent ATO Memo for the FHFA GSS was signed on September 12, 2018.