Privacy Impact Assessment Template

OFFICE OF INSPECTOR GENERAL NETWORK (OIGNet) GENERAL SUPPORT SYSTEM (GSS)
(SYSTEM NAME)

MARCH 8, 2018
DATE

FHFA-OIG's Chief Counsel handles certain tasks commonly undertaken by an agency's Senior Agency Official for Privacy (SAOP). This template is used when FHFA-OIG's Chief Counsel determines that an FHFA-OIG IT System contains Personally Identifiable Information and a more in-depth assessment is required.

Complete and sign this template and forward to the FHFA-OIG Chief Counsel for review and coordination with the agency SAOP.

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-OIG: 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 FHFA-OIG's IT developers, IT security officers, and Office of Counsel.

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 FHFA-OIG Chief Counsel may make a determination that a complete PIA is not necessary depending upon the nature and extent of the PII collected. When the Chief Counsel 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-OIG 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 FHFA-OIG Office of Counsel for assistance.

SECTION 2.0 USES OF THE INFORMATION

- Identify the primary uses of the information and how the information supports FHFA-OIG'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-OIG manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule, to which FHFA-OIG is subject. For the data being created/ maintained in the System, these records schedules are the authoritative sources for this information. For assistance, contact FHFA-OIG's Office of Administration (OAd).
- 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-OIG's Office of Counsel.
- 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.
- FHFA-OIG is subject to FHFA's agency-specific Privacy Act Rule published 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. "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-OIG 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-OIG, 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.
- 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: March 8, 2018

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
David Bonorchis	David.Bonorchis@fhfaoig.gov	FHFA-OIG OAd/IT	202-730-0362

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

The Office of Inspector General Network (OIGNet) General Support System (GSS) is a general purpose, multi-user system used throughout FHFA-OIG. The OIGNet GSS is not a database or database management system and is composed of users with desktops, laptops, tablets and other ancillary equipment connected via the FHFA-OIG backbone network to central servers that support FHFA-OIG.

The OIGNet GSS was developed with state-of-the-art components with the focus of providing FHFA-OIG a network infrastructure that allows all staff members to perform their designated roles and responsibilities. This was done by sourcing a network infrastructure with a small footprint while outsourcing services with cloud computing technology.

The OIGNet GSS includes transmittal of the following types of information:

1. Employee personnel information generated throughout the human resources process.
2. Personal information provided by individuals making Freedom of Information Act requests and Privacy Act requests, and personal information submitted through public inquiries to FHFA-OIG.
3. Federal and business partner information may potentially be processed, stored, and/or transmitted at any given time through the various applications and components connected via the system.
4. Other identifying information that FHFA-OIG may possess in its day-to-day operations that may at times be of a sensitive nature.

Although various components in the OIGNet GSS may contain PII, the system does not function as a group of records from which information is retrieved by the name of an individual, or by any number, symbol, or other unique identifier assigned by the system to that individual.

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?	In the FHFA-OIG Active Directory environment: name, business address and phone numbers, business e-mails; and FHFA-OIG-provided asset information for FHFA-OIG employees, contractors, and authorized users. No PII from the public is collected, used or stored by the OIGNet GSS.

#	Question	Response
1.2	What or who are the sources of the information in the System?	The source for the information can be directly from the individual, from FHFA-OIG Human Resources, and/or IT Support.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The information is necessary to track and maintain computer assets and locations of and contact methods for FHFA-OIG employees.
1.4	How is the information provided to FHFA?	The information is collected from the Office of Administration (OAd) hiring and on-boarding documentation when employees first arrive and are provided government furnished equipment. Once an administrator has the information, it is then entered in Active Directory.
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.	The risk to an individual's privacy is the loss or compromise of one's business contact information and any additional contact information entered by the IT Support staff or voluntarily entered by the employee into Active Directory.
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: Social Security numbers are not collected.

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 use of the information is to maintain accountability of equipment and contact information for the employees and contractors of FHFA-OIG.
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 control to FHFA-OIG information systems is managed through Microsoft Active Directory security groups to ensure that users are granted access based on group membership to only those network resources, OIGNet GSS, or individual FHFA-OIG application services in the information system inventory for which the users have an approved need based on their assigned duties. All access rights may be approved by the user's supervisor/manager, system owner, or IT Support. The authorized IT Support personnel make the approved access control changes to Active Directory users, groups, and FHFA-OIG applications.

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?	See 3.2
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.	All FHFA-OIG records are subject to FHFA's Comprehensive Records Schedule. The OIGNet GSS may contain a variety of records, subject to varied retention periods. Potential disposition of records maintained in the OIGNet GSS must be evaluated on a case-by-case basis to determine the appropriate retention period for each record.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Current and disabled accounts may remain indefinitely to facilitate legal or agency review of account information.

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 for the OIGNet GSS. While the OIGNet GSS as a support system passes information in and out of FHFA-OIG's network and connects various systems, the OIGNet GSS is not a system of record itself. It authenticates and allows users to connect to the FHFA-OIG network and does not retrieve information through a personal identifier. Personal information and records provided to FHFA-OIG through FOIA or Privacy Act requests or that are otherwise submitted to FHFA-OIG are not stored, maintained, or retrieved by the OIGNet GSS itself through a personal identifier. FHFA-OIG publishes SORNs for the specific systems applicable to the storage, maintenance, and retrieval of any personal information provided by the public. The OIGNet GSS is not a database or database management system and although various components may contain PII, the OIGNet GSS does not function as a group of records from which information is retrieved by the name of an individual, or by any number, symbol, or other unique identifier assigned by the system to that individual.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	No. The information is received from FHFA-OIG OAd Human Resources and is only for business purposes, or information is voluntarily provided and/or updated by individuals.
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?	FHFA-OIG OAd Human Resources must acquire the information for employee onboarding and is used for agency business purposes such as internal contact information and network access.

#	Question	Response
4.4	What are the procedures that allow individuals to gain access to their information?	The information is received from FHFA-OIG OAd Human Resources and is only for business purposes (i.e. business address, business telephone numbers, and business email addresses). FHFA-OIG users can access the Active Directory to review their information at any time and facilitate necessary changes with FHFA-OIG OAd IT.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Onboarding procedures are used by FHFA-OIG OAd Human Resources to acquire work related information for all employees.

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?	Business contact information is shared with other internal users through Global Address List for purposes of conducting FHFA-OIG work.
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	The information is not shared by the system with any external organization including Federal, state, local government, and private sector.
5.3	Is the sharing of PII outside FHFA-OIG 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-OIG.	PII records maintained in the various components connected by the OIGNet GSS may be shared and, as applicable, are covered by an appropriate routine use in a SORN that is applicable to the specific component or application.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	No external sharing is performed by the OIGNet GSS. PII records maintained in the various components connected within the OIGNet GSS are covered by an appropriate routine use in a SORN relating to the specific component or application, and privacy risks are managed through the individual applications and components.

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 Chief Counsel with this PIA.**	All FHFA-OIG users are required to consent to FHFA-OIG's IT Rules of Behavior to gain access to the system.
6.2	Will non-FHFA-OIG 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 FHFA-OIG control their access and use of information? Are there procedures documented in writing? **If so, provide a copy to the Chief Counsel with this PIA.**	Limited non-FHFA-OIG personnel, including contractor personnel, may access the OIGNet GSS. Access is gained and controlled by the user consenting to FHFA-OIG's IT Rules of Behavior.
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?	In accordance with FHFA-OIG Security Awareness Training, all FHFA-OIG system users are required to have initial and recurring annual security awareness training to commensurate with their system responsibilities. All system administrators receive privileged account user training
6.4	Describe the technical/administrative safeguards in place to protect the data?	FHFA-OIG implements the following controls to protect the integrity and confidentiality of information transmitted across internal and external networks: • Two-factor authentication is required via use of an HSPD-12 PIV card and PIN. • Secure network access to agency resources is provided through encrypted virtual private network (VPN) connections across public networks. In addition, the FHFA-OIG network infrastructure is connected to the internet for VoIP phone services, and a MTIPS line for dataservices. • The FHFA-OIG system administrator uses a secure protocol for secure login to network devices. • SSL protocol provides encrypted transmission for web based applications.

#	Question	Response
		• Hard disk encryption is used on all FHFA-OIG workstations (Desktops, laptops, and tablets).
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Audits, in accordance with NIST (SP) 800-53A, are performed with prescribed frequency to validate that the methods to protect FHFA-OIG infrastructure and information systems are employed, implemented, and performed in a consistent manner. Security events are logged and correlated as part of FHFA-OIG continuous monitoring.
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 OIGNet GSS SA&A was completed March 22, 2017.
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 Chief Counsel with this PIA.** If not, when do you anticipate such ATO being issued?	The most recent ATO was issued for the GSS on March 22, 2017 with an ongoing authorization in accordance with documented continuous monitoring activities and in alignment with the Office of Management and Budget Circular A-130.

Signatures

FHFA-OIG:

David Bonorchis
System Owner (Printed Name)

System Owner (Signature)

3/13/2018
Date

N/A
Executive Sponsor (Printed Name)

Executive Sponsor (Signature)

Date

N/A
System Developer (Printed Name)

System Developer (Signature)

Date

Michael Stoner
Chief Information Security Officer (Printed Name)

Chief Information Security Officer (Signature)

3/13/18
Date

Michael Smith
Chief Information Officer
(Printed Name)

Michael Smith
Chief Information Officer
(Signature)

3/13/18
Date

Leonard J. DePasquale
Chief Counsel
(Printed Name)

Chief Counsel
(Signature)

3-14-18
Date

FHFA:

David A. Lee
Senior Agency Official for Privacy
(Printed Name)

Senior Agency Official for Privacy
(Signature)

3/15/2018
Date