Modified Privacy Impact Assessment Template

MODIFIED GENERAL SUPPORT SYSTEM (GSS) TO INCLUDE

AZURE ACTIVE DIRECTORY (AD) SYNCHRONIZATION
(SYSTEM NAME)

7/28/2017
DATE

This Modified Privacy Impact Assessment Template is used when the Senior Agency Official for Privacy determines that an IT System contains Personally Identifiable Information and an 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 20219
(202) 649-3803
Privacy@fhfa.gov

Guidance for Completing the Modified 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. Executive Sponsors, System Owners and Developers are responsible for completing the PIA.

The guidance below has been provided to help 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 MODIFIED PIA COMPLETE THE FOLLOWING SECTIONS:

- **Overview**
- **Sections 1, 2, 3 and 4**

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 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.

MODIFIED 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: July 28, 2017

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Thomas 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.			
FHFA's Office of Technology and Information Management (OTIM) is in the process of evaluating cloud services from Microsoft including advanced email filtering and protection. In order to leverage all of the capabilities, FHFA's Active Directory (AD) attributes need to be synchronized with Microsoft Azure. FHFA will not implement password synchronization as part of this process.			

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?	accountEnabled accountName assistant authOrig c

#	Question	Response
		cn co company countryCode dLMemRejectPerms dLMemSubmitPerms department description deviceId deviceOSType deviceOSVersion deviceTrustType displayName domainFQDN domainNetBios extensionAttribute1 extensionAttribute10 extensionAttribute11 extensionAttribute12 extensionAttribute13 extensionAttribute14 extensionAttribute15 extensionAttribute2 extensionAttribute4 extensionAttribute5 extensionAttribute6 extensionAttribute7 extensionAttribute8 extensionAttribute9 facsimileTelephoneNumber

#	Question	Response
		givenName hideDLMembership info initials ipPhone l legacyExchangeDN mail mailNickname managedBy manager member memberCount middleName mobile msDS-HABSeniorityIndex msDS-PhoneticDisplayName msExchArchiveGUID msExchArchiveName msExchAssistantName msExchAuditAdmin msExchAuditDelegate msExchAuditDelegateAdmin msExchAuditOwner msExchBlockedSendersHash msExchBypassAudit msExchCoManagedByLink msExchDelegateListLink msExchELCExpirySuspensionEnd msExchELCExpirySuspensionStart

#	Question	Response
		msExchELCMailboxFlags msExchEnableModeration msExchExtensionCustomAttribute1 msExchExtensionCustomAttribute2 msExchExtensionCustomAttribute3 msExchExtensionCustomAttribute4 msExchExtensionCustomAttribute5 msExchHideFromAddressLists msExchImmutableId msExchLitigationHoldDate msExchLitigationHoldOwner msExchMailboxAuditEnable msExchMailboxAuditLogAgeLimit msExchMailboxGuid msExchModeratedByLink msExchModerationFlags msExchRecipientDisplayType msExchRecipientTypeDetails msExchRemoteRecipientType msExchRequireAuthToSendTo msExchResourceCapacity msExchResourceDisplay msExchResourceMetaData msExchResourceSearchProperties msExchRetentionComment msExchRetentionURL msExchSafeRecipientsHash msExchSafeSendersHash msExchSenderHintTranslations msExchTeamMailboxExpiration

#	Question	Response
		msExchTeamMailboxOwners msExchTeamMailboxSharePointLinkedBy msExchTeamMailboxSharePointUrl msExchUserHoldPolicies msOrg-IsOrganizational msRTCSIP-ApplicationOptions msRTCSIP-DeploymentLocator msRTCSIP-Line msRTCSIP-OptionFlags msRTCSIP-OwnerUrn msRTCSIP-PrimaryUserAddress msRTCSIP-UserEnabled oOFReplyToOriginator objectSid onPremisesUserPrincipalName otherFacsimileTelephoneNumber otherIpPhone otherMobile otherPager otherTelephone pager physicalDeliveryOfficeName postOfficeBox postalAddress postalCode preferredLanguage proxyAddresses publicDelegates pwdLastSet registeredOwnerReference

#	Question	Response
		reportToOriginator reportToOwner securityEnabled sn sourceAnchor st streetAddress targetAddress telephoneAssistant telephoneNumber thumbnailPhoto title unauthOrig url usageLocation userCertificate userPrincipalName userSMIMECertificate wWWHomePage
1.2	What are the sources of the information in the System?	Employees Human Resources Facilities Management Information Technology Operations
1.3	Why is the information being collected, used, disseminated, or maintained?	Synchronization of Active Directory attributes to Microsoft Azure is necessary to take advantage Microsoft cloud services such as Exchange Online Protection (EOP).
1.4	How is the information collected?	The information will be loaded from the FHFA Active Directory where the information is derived from other data where a privacy act statement was provided. The information is collected from FHFA offices including Human Resources, Facilities Management and IT.

#	Question	Response
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	The PII elements, including name, work address, 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.

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 information will be used to provide a common identity for FHFA users when leveraging Office 365 applications.
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 the data is limited to those with an operational need to access the information. This includes enrollment personnel, management and system owners.

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?	FHFA uses Veritas Enterprise Vault (Evault) for the management of permanent and temporary electronic records. As part of this, FHFA uses a quarterly Evault migration process and procedures. Information in this system will be migrated to Evault, validated, and then deleted from this system within 120 days after termination or separation of an employee or contractor personnel.
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.	Records pertaining to the management of this system will be managed in the Evault in accordance with FHFA's Comprehensive Records Schedule (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.	Risks are minimal given that records are destroyed relatively soon after an employee/contractor personnel departs FHFA. However, in order to

#	Question	Response
		mitigate any risks, OTIM will work with Records and Information Management (RIM) to document and approve disposition activity on records that have been migrated into Evault.

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.	OTIM has completed Access Control and Audit Procedures which describe the process for approving, creating and deactivating privileged Office 365 user accounts.
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.	Only authorized OTIM employees and contractors will have privileged access to Office 365. Privileged users must be granted a specific role as described in the Access Control and Audit Procedures.
6.3	Describe the training that is provided to users either generally or specifically that is relevant to the program or System?	Privileged users are provided with the Access Control and Audit Procedures which define best security practices for administering Office 365 accounts.
6.4	What technical safeguards are in place to protect the data?	Office 365 Multi-Tenant & Supporting Services and Microsoft Azure Cloud has been authorized by FedRAMP at the Moderate Impact level.
6.5	What auditing measures are in place to protect the data?	Office 365 audits all administrator activity. Audit reports are available to administrators as needed.

#	Question	Response
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.	FHFA has reviewed the FedRAMP package for Office 365 Multi-Tenant & Supporting Services and Azure Cloud and will issue an agency ATO. This is expected to be completed by July 26, 2017.

Signatures

Thomas Leach
System Owner (Printed Name) — System Owner (Signature) — 7/31/2017 Date

Thomas Leach
Executive Sponsor (Printed Name) — Executive Sponsor (Signature) — 7/31/2017 Date

James Vercellone
System Developer (Printed Name) (as applicable) — System Developer (Signature) — 7/31/2017 Date

Ralph Mosios
Chief Information Security Officer (Printed Name) — Chief Information Security Officer (Signature) — 7/31/2017 Date

Kevin Winkler
Chief Information Officer (Printed Name) — Chief Information Officer (Signature) — 7/31/2017 Date

David A. Lee
Senior Agency Official for Privacy (Printed Name) — Senior Agency Official for Privacy (Signature) — 8/1/2017 Date