



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

- 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.

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 <u>not</u> 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

FHFA PIA Microsoft Office 365 AD Synchronization

#	Question	Response
		<p>givenName hideDLMembership info initials ipPhone 1 legacyExchangeDN mail mailNickname managedBy manager member memberCount middleName mobile msDS-HABSeniorityIndex msDS-PhoneticDisplayName msExchArchiveGUID msExchArchiveName msExchAssistantName msExchAuditAdmin msExchAuditDelegate msExchAuditDelegateAdmin msExchAuditOwner msExchBlockedSendersHash msExchBypassAudit msExchCoManagedByLink msExchDelegateListLink msExchELCEpirySuspensionEnd msExchELCEpirySuspensionStart</p>

FHFA PIA Microsoft Office 365 AD Synchronization

#	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
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
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.

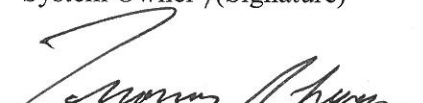
Signatures

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