



Privacy Impact Assessment Template

OCO STATUS TRACKING AND REPORTING (STAR) **(SYSTEM NAME)**

This template is used when the Chief Privacy Officer determines that the 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
1700 G Street NW
Washington, DC 20552
(202) 414-3804
David.Lee@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form (IIF) 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 IT system?
 - What will be the primary uses of the system?
 - How will this support the 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
- Section 1
- Section 2
- Section 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 include:
 - 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 an organization).
- If the system collects information from 10 or more members of the public, ensure that the agency has received OMB prior approval 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 the Agency's or 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 of 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, the 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 personal 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 Privacy Act Officer. The Privacy Act requires that any amendments to an existing system must also be addressed in a Federal Register notice.
- If a name or other personal 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 systems 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 it is unknown 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 the Inspector General. "Other" may also include database administrators or IT Security Officers. Also include

organizations listed in the Privacy Act system of records notice under the “Routine Use” section when a Privacy Act system of records notice 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 that 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 Technical Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.
- The IT Security Certificate and Accreditation (C&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 C&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: 1/20/12

Name of System: OCO STAR

System Owner(s)(including Division/Office): Mary Johnson, OCO

Name	E-mail	Phone #
Mary Johnson	Mary.Johnson@fhfa.gov	202-649-3043

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 OCO STAR system automates OCO’s weekly status report, which lists and tracks all issues for which the Enterprises are requesting FHFA action as Conservator from the initial request date to the closure date. As this system was designed to track requests from the Enterprises while in conservatorship, it links directly to FHFA’s mission as conservator. The system is accessible to Enterprise users (currently only 4 have been granted access) through FHFA’s extranet (each Enterprise can only access information related to their own company). There are 5 OCO administrators for the system: Mary Johnson, Philip Anderson, Robert Keyes, Brad Martin, and Owen Highfill. In addition, there are other FHFA staff who have access (they have more limited access than OCO admins). They are either the “responsible official” or the “primary contact” listed for each issue on the status report. There are also Policy and OPAR administrators who will also have limited access, but will be able to add/close issues as appropriate in their designated areas. All users are able to add comments to existing issues, but OCO admins have to approve any changes or additions before they are posted in the application. The system generates weekly reports of open or closed policy or conservatorship issues, listed in order of priority. Users can also generate reports listed in order of FHFA responsible official.

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 personally identifiable information (PII), such as name, address, social security number, date of birth, financial information, etc.

FHFA PIA FOR OCO STAR
(System Name)

#	Question	Response
1.1	What information is collected, used, disseminated, or maintained in the system?	The information in the system is all related to tracking conservatorship requests. That information includes the requests from the Enterprises, updates/comments on the request from both FHFA and the Enterprises, and the final response to the request from FHFA. This information is collected, along with the names of any contacts from the Enterprises and FHFA who are working on an issue. The information is disseminated when users generate reports from the system. This information is downloaded into a spreadsheet that can then be shared with other Enterprise and FHFA staff.
1.2	What are the sources of the information in the system?	Information is gathered from entries from FHFA and Enterprise users on the status of requests and from information pulled from emailed conservator requests sent to FHFA_Conservator_Decision@fhfa.gov .
1.3	Why is the information being collected, used, disseminated, or maintained?	The information is being collected and used to track requests from the Enterprises to FHFA that require conservator review and approval.
1.4	How is the information collected?	The Enterprises users gather information from the business units and adds comments to the system. FHFA collects information from the FHFA_Conservator_Decision@fhfa.gov email box and from comments added by FHFA users working on the requests.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	In general, personal information is not entered into the system; however, users' email address or other information attached to a request may be entered into the system. That information could then only be viewed by users of the system, which to date include 4 Enterprise staff and a limited number of FHFA staff.

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 is used to track the progress of conservatorship requests and to update the Enterprises/FHFA on the status of requests.
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.	During training, users are informed that the application is not a system of record and that the information entered is viewable by both FHFA and Enterprise users. OCO staff explain the

FHFA PIA FOR OCO STAR
(System Name)

#	Question	Response
		purpose of the tracking system during the training as well. Before users can access the application, they must agree to the terms of use that explains that the system can only be access by authorized users and that using the information for anything other than official government purposes is prohibited.

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?	N/A
3.2	Has a retention schedule been approved by the Agency's Records Management Officer and NARA? If yes, provide the corresponding GRS or Agency specific Records Schedule number.	N/A
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	N/A

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.	N/A
4.2	Was notice provided to the individual prior to collection of information?	N/A
4.3	Do individuals have the opportunity and/or right to decline to provide 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?	N/A
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.	N/A
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? If so, describe. If not, describe under what legal authority the program or system is allowed to share PII outside of the agency.	N/A
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	N/A

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

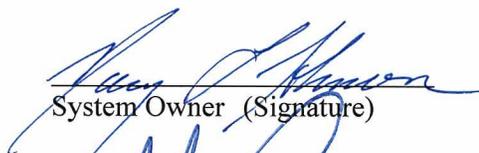
#	Question	Response
6.1	What procedures are in place to determine which users may access the system? Are these procedures documented in writing? If so, attach a copy to this PIA.	Agency executives and managers whose offices contribute to conservatorship decisions and who were on the distribution list for the weekly emailed status report (prior to 2012) were originally given access to the system. For additional FHFA staff to receive access, an executive/manager must request it from OCO. Any Enterprise user must complete an application access request form and submit it to OCO who will then make a request through the Help Desk that access be given. These procedures are not documented in writing.

FHFA PIA FOR OCO STAR
(System Name)

#	Question	Response
6.2	Will contractors have access to the system? If yes, how will contractors 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.	No.
6.3	Describe the training that is provided to users either generally or specifically relevant to the program or system?	OCO provides training to all users, which includes an overview of the system and demonstration. OCO will also provide specific training to different user groups as needed.
6.4	What technical safeguards are in place to protect the data?	This information is stored on FHFA's internal production SQL Server, located behind our firewall. Authentication is provided through Windows integrated Kerberos authentication. System access is controlled through Active Directory security groups.
6.5	What auditing measures are in place to protect the data?	All access to the OCO STAR system is audited into Audit Central. This provides the user id, timestamp, IP address and actions performed by the user during the session.
6.6	Has a C&A been completed for the system or systems supporting the program? If so, provide the date the last C&A was completed.	No. This system falls under the General Support System.

Signatures

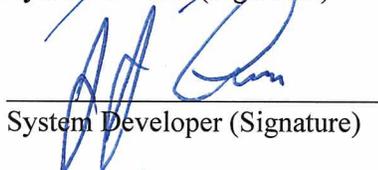
Mary Johnson
System Owner (Printed Name)



System Owner (Signature)

1/20/2012
Date

Jude Corina
System Developer (Printed Name)



System Developer (Signature)

1/23/2012
Date

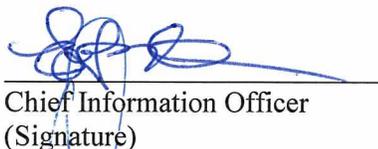
Ralph Mosios
Chief Information Security Officer
(Printed Name)



Chief Information Security Officer
(Signature)

1/23/2012
Date

R. Kevin Winkler
Chief Information Officer
(Printed Name)



Chief Information Officer
(Signature)

1/23/2012
Date

David A. Lee
Chief Privacy Officer
(Printed Name)



Chief Privacy Officer
(Signature)

1/24/2012
Date