Privacy Impact Assessment Template

OFFICE OF INSPECTOR GENERAL CASE MANAGEMENT SYSTEM (CMS) (OIG CMS)

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.

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 such as Neighborworks).
- 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 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 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: July 27, 2012

Name of System: FHFA-OIG Case Management System

System Owner(s)(including Division/Office): Office of Inspector General, Federal Housing Finance Agency

Name	E-mail	Phone #
Peter Emerzian	peter.emerzian@fhfaoig.gov	202.730.4751

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 purpose of this system is to maintain the following types of information: (1) complaints received by FHFA-OIG, including those from individuals and their representatives, oversight committees, and others who conduct business with FHFA-OIG; (2) information relevant to efforts to resolve those complaints; (3) information collected as part of investigations conducted by FHFA-OIG's Office of Investigations (OI); (4) correspondence specific to investigations received by FHFA-OIG from individuals and their representatives, oversight committees, and others who conduct business with FHFA-OIG, and the responses thereto.

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.

#	Question	Response
1.1	What information is collected, used, disseminated, or maintained in the system?	CMS is designed to facilitate the organization and development of criminal investigations by OIG. Depending on the nature of the complaint or investigation, CMS may store the name, address, social security number, birthdate, financial account information or other personal information about a complainant or investigatory target.
1.2	What are the sources of the information in the system?	The information may derive from named or anonymous complaints or tips from the general public – either through the OIG Hotline or directly to OIG, Congressional members or staff, or FHFA or GSE employees. Additional information will emerge from resulting investigations.
1.3	Why is the information being collected, used, disseminated, or maintained?	The information is necessary to build criminal and civil cases against individuals for violations of federal laws or regulations. The information is also retained for searches for similar crimes in future cases.
1.4	How is the information collected?	In the case of telephone hotline tips/complaints, the information is collected by hotline personnel at the National Center for Disaster Fraud in Baton Rouge, Louisiana. Other information will be collected by personal or telephonic interviews, and entered by hand into CMS by OIG special agents or investigative staff.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	Risks to an individual's privacy are that their personal, financial and other information may be subject to disclosure and compromise, as well as the fact that they are or potentially are the subject of a criminal or civil investigation by the OIG, or some other law enforcement entity.

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.	See Section 1.3
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.	The system is maintained on OIG-dedicated secure physical servers, hosted at NASA-OIG headquarters in Washington, DC. For OIG personnel to access the system, they are issued an RSA token by NASA to gain access to the CMS server. In addition to using the RSA token, the user must provide a log-on name, an 8-digit unique PIN, the RSA token value (which changes every 60 seconds), and a minimum 12 character password requiring special characters, capital letters, and numbers. In addition, users are identified with session-specific IP addresses, such that the same username cannot be used simultaneously from another location, and if the user's session times out without a proper log-off procedure, the user will be denied access for 8 hours from any other location.

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?	Pursuant to the FHFA Records Retention Schedule (5-30-11), **Significant Investigative and Evaluative Case Records** are retained permanently. The records are transferred to NARA 30 years after cutoff (when the activity is completed or superseded). **Investigative and Evaluative Case Records** are deemed temporary, and either destroyed or deleted 15 years after cutoff. **Investigative and Evaluative Non-Case Records** are deemed temporary, and are destroyed or deleted three (3) years after cutoff.

#	Question	Response
		Detailed definitions of each type of record can be found in Section 7 of the FHFA Records Retention Schedule (5-30-11).
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.	As noted, in Section 3.1, FHFA-OIG follows the FHFA Records Retention Schedule, which is currently under review by NARA.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Risks from the retention of data are identical to those associated with current information; accordingly, protections against breaches of privacy are in place (see section 2.2 for detail). Additionally, requests for CMS information from other OIG staff must be cleared by a Deputy Inspector General. Finally, to access any information used in a grand jury matter, the requester must produce an authorization pursuant to the Federal Rules of Criminal Procedure.

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.	FHFA-OIG published a SORN on March 2, 2011 in the Federal Register, covering five systems of records: FHFA-OIG Audit Files Database, FHFA-OIG Investigative & Evaluative Files Database, FHFA-OIG Investigative & Evaluative MIS Database, FHFA-OIG Hotline Database, and FHFA-OIG Correspondence Database. CMS will consolidate and replace the systems above with certain exceptions, *i.e.*, FHFA-OIG Audit Files Database will remain separate, and Evaluative Files will not be included in CMS. Either a new SORN will be issued, or the current SORNs will be amended to cover CMS specifically.
4.2	Was notice provided to the individual prior to collection of information?	Hotline and other complainants are given the option of how much personal information they choose to provide. Investigative subjects or targets are not notified of the collection of information, because of the risks of evidence destruction and witness tampering.

#	Question	Response
4.3	Do individuals have the opportunity and/or right to decline to provide information?	As noted in Section 4.2 above, complainants determine how much information they wish to provide; and subjects or targets do not have such opportunity.
4.4	What are the procedures that allow individuals to gain access to their information?	FHFA has issued Freedom of Information Act (FOIA) and Privacy Act regulations that address the production and release of OIG records. These regulations cover requests for investigative files by both complainants and potential targets; responses are implemented pursuant to FOIA and the Privacy Act of 1974.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Information is inputted and maintained by the case agent. As part of their duties, the information is required to be both up-to-date and accurate. Any discrepancies or errors identified can and will be corrected by the case agent. Further, the proper maintenance of files and data accuracy are elements of the performance review process for OIG special agents. For an individual who requests a correction to his Privacy Act information, OIG will follow the procedures documented in the FHFA Privacy Act regulation.

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?	Case information may be shared with the OIG Offices of Audits and Evaluations. The information shared may encompass the entire case file, depending on the requirements of the individual request. The requests are often made to ensure that OIG efforts are not duplicated and the law enforcement activity is not compromised by inadvertent disclosure during the conduct of an audit or evaluation.

#	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.	Case information may be shared with other law enforcement agencies, including U.S. Attorneys offices, state prosecutors, or any state or federal law enforcement agencies (including OIGs) with whom a joint investigative is being conducted. Other releases may be to the general public or media, pursuant to the FOIA. All releases under the FOIA include the proper redactions under 5 U.S.C. § 552(b).
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.	Yes. Yes. Currently, OIG shares PII in accordance with the routine uses set forth in the SORNs.
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	Risks (as described in section 1.5) are that when shared with an external source, the data may be comprised by that external source, either inadvertently through a breach, or other compromise, or the information is deliberately released. Open case information from CMS is shared with other law enforcement entities with existing PII control and protection infrastructures, i.e., Department of Justice. All information transferred is done so with the notification that the material may not be disclosed without the prior authorization of OIG. Closed case file information is only disclosed to authorized recipients on-site at OIG – the material cannot be removed or copied without OIG permission. The viewing party submits a written acknowledgement of OIG's control over any disclosure of the information. This acknowledgement is made part of the case file.

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.	Access to CMS is restricted to authorized users. Those authorized users are identified by the Deputy Inspector General for Investigations, and are limited to special agents, investigative counsel, or investigative support staff within OI. Access procedures are documented in the OIG OI Policy and Procedures Manual (Section 4.15). The relevant text of the section currently reads: Proper case file preparation and organization is necessary to document the investigative work performed and to provide adequate support for findings developed as a result of an investigation. The official OI file pertaining to a particular investigation is referred to as the Official Case File (OCF) located in the CMS. OCFs are to be maintained in the secure CMS Server and accessible only through proper login and authentication established by OI. Access to the OCF is on a "need to know" basis and will typically be restricted to the OI staff or, in sensitive matters, limited only to the case agent and SAC. With the exception of investigations identified as "Confidential", all OI staff have read-only access to all information contained in the CMS. Write access is granted to OI staff listed in the Staff Tab within each investigation, which is controlled and managed by the assigned case agent or the systems administrator. By default, supervisorial access is granted within the Staff Tab through the automatic population of the tab listing only those case supervisors. All OI OCFs are accessible through authorized, secure access only. The OCF is to be organized, managed, and maintained by the assigned

#	Question	Response
		SA.
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.	Contractors do not have access to CMS presently. Future needs will determine any changes to the access policy, which would be approved by the Deputy Inspector General for Investigations.
6.3	Describe the training that is provided to users either generally or specifically relevant to the program or system?	User training is conducted upon assignment to the Office of Investigation, and lasts approximately 3 hours. This training includes assignments of passwords and RSA token and log-on information. Users are also trained on how to safely and securely access information in the CMS. Ongoing training will be conducted on a regular basis, no later than annually.
6.4	What technical safeguards are in place to protect the data?	See Section 2.2 for detailed technical information on controls and safeguards.
6.5	What auditing measures are in place to protect the data?	Audit controls for system access are in place at NASA Headquarters. Within CMS, changes to data are documented with the time, user, and nature of the change. Additionally, for certain interview documents, any changes are provisional until approved by an OI manager.
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.	A C&A for the secure hosting and storage facility at NASA was last completed on September 29, 2010. FHFA issued an Authorization to Operate for CMS on December 16, 2011. Since CMS' installation, follow-up C&A items specific to CMS are being reviewed and documented.

Signatures

Peter Emorsian
System Owner (Printed Name)

System Owner (Signature)

7/27/12
Date

Randal A Stewart
System Developer (Printed Name)

System Developer (Signature)

7-30-12
Date

For David Brockus
Bill Smith
Chief Information Security Officer
(Printed Name)

Chief Information Security Officer
(Signature)

7/28/12
Date

Chief Information Officer
(Printed Name)

Chief Information Officer
(Signature)

7/30/12
Date

David A. Lee
Chief Privacy Officer
(Printed Name)

Chief Privacy Officer
(Signature)

7/30/2012
Date