Privacy Impact Assessment Template

FOIAEXPRESS
(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: I) 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)(l).
- 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:

Name of System:

System Owner(s) (including Division/Office):

Name	E-mail	Phone#
Stacy J. Easter	Stacy.easter@fhfa.gov	202-414-3762

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.

To assist FHF A in receiving, processing, and tracking FOIA and Privacy Act requests from the public.

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?	Name, contact information (i.e. address, email and phone numbers), and other identifying information provided by the requester.
1.2	What are the sources of the information in the system?	Directly from the individuals providing the information.
1.3	Why is the information being collected, used, disseminated, or maintained?	In order to facilitate the processing of requests and in order to contact and communicate with the requester.
1.4	How is the information collected?	Through a web based application, e-mail, fax, and U.S. mail.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	The risk to an individual's privacy are the loss or compromise of their contact information.

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.	To track, and contact requesters. Also, information may be used to verify someone's identity for a privacy act request.
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.	SSL encryption for data transmission. Limited access to back end database (only 4 software licenses). Protected by being part of FHFA's GSS system.

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?	Minimum 2 years and up to 6 years 3 months after requests are closed.
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.	Yes. GRS-14
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The risks associated with the length of time are that information is maintained for up to 6 years which means it is susceptible to loss or compromise over a significant period of time. Such risks are mitigated by limited access, password controls, logging activities, etc. to monitor access to 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.	Yes. FHFA-13 (attached).
4.2	Was notice provided to the individual prior to collection of information?	Yes.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes.
4.4	What are the procedures that allow individuals to gain access to their information?	They are set forth in the SORN - FHFA-13.

#	Question	Response
4.5	What are the procedures for correcting inaccurate or erroneous information	They are set forth in the SORN - FHFA-13.

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?	All offices in FHFA. The information shared is generally just the nature of the request. Personal information is not shared unless it is a privacy act request.
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.	Other Federal agencies if referring a request or seeking consultation on a request. All information, including personal information.
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. The routine uses are set forth in the SORN - FHFA-13.
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	Privacy risks are the loss of information. They are mitigated by mailing information or emailing, with password protected files.

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.	There are no written procedures in place. Access is limited to FOIA personnel and IT administrator for administrative support.

#	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.	Possibly. They will access it as IT contractor support personnel or in the event FHFA hires a contractor to provide FOIA or Privacy Act processing support. Their access is controlled by the software administrator. Their use is restricted by FHFA rules of behavior.
6.3	Describe the training that is provided to users either generally or specifically relevant to the program or system?	Training is provided by the vendor.
6.4	What technical safeguards are in place to protect the data?	Data is stored in a password protected database, on a clustered Microsoft SQL 2008 R2 server.
6.5	What auditing measures are in place to protect the data?	None.
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. Not applicable.

Stacy Easter System Owner (Printed Name)	System Owner (Signature)	11/17/2011 Date
N/A - COTS System Developer (Printed Name)	System Developer (Signature)	Date
Ralph Mosios Chief Information Security Officer (Printed Name)	Chief Information Security Officer (Signature)	11/21/2011 Date
R. Kevin Winkler Chief Information Officer (Printed Name)	Chief Information Officer (Signature)	11/22/11 Date
David A. Lee Chief Privacy Officer (Printed Name)	Chief Privacy Officer (Signature)	12/1/2011 Date

formation of car pools with employees who have been issued parking permits, and to provide for the safe use of FHFA facilities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside FHFA as a routine use as follows:

(1) To appropriate federal, state, and local authorities responsible for investigating or prosecuting a violation of, or for enforcing or implementing a statute, rule, regulation, or order issued, when the information indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto;

(2) To a court, magistrate, or other administrative body in the course of presenting evidence, including disclosures to counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal proceedings, when FHFA is a party to the proceeding or has a significant interest in the proceeding, to the extent that the information is determined to be relevant and necessary.

(3) To a congressional office in response to an inquiry made by the congressional office at the request of the individual who is the subject of the record;

(4) To appropriate federal, state, local authorities, and other entities when (a) It is suspected or confirmed that the security or confidentiality of information in the system has been compromised; (b) there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs that rely upon the compromised information; and (c) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(5) To appropriate federal, state, and local authorities in connection with hiring or retaining an individual, conducting a background security or suitability investigation, adjudication of liability, or eligibility for a license, contract, grant, or other benefit;

(6) To appropriate federal, state, and local authorities, agencies, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or corrective actions or grievances or appeals, or if needed in the performance of other authorized duties;

(7) To appropriate federal agencies and other public authorities for use in records management inspections;

(8) To officials of a labor organization when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions;

(9) To contractor personnel,, grantees, volunteers, interns, and others performing or working on a contract, service, grant, cooperative agreement, or project for the Federal Government; and

(10) To government and commercial vendors that provide parking-related services and systems involving FHFA employees.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained in paper form, electronic format, and magnetic disk or tape. Electronic records are stored in computerized databases. Paper and magnetic disk or tape records are stored in locked file rooms or locked file cabinets.

retrievability:

Records are indexed and retrieved by employee name, employee identification number, license tag number, or by other personal identifier .

SAFEGUARDS:

Records are safeguarded in a secured environment. Buildings where records are stored have security cameras and 24-hour security guard service. Access is limited to those individuals whose official duties require access. Computerized records are safeguarded through use of access codes and other information technology security measures.

RETENTION AND DISPOSAL:

Paper records and electronic media are retained in accordance with National Archives and Records Administration and FHFA Records Retention and Disposition Schedules. Disposal is by shredding or other appropriate disposal systems.

SYSTEM MANAGER(S) AND ADDRESS:

Office of Human Resources Management, Federal Housing Finance Agency, 1625 Eye Street, NW., Washington, DC 20006.

NOTIFICATION PROCEDURE:

Direct inquiries as to whether this system contains a record pertaining to an individual to the Privacy Act Officer, Federal Housing Finance Agency, 1700 G Street, NW., Washington, DC 2052, or *privacy@fhfa.gov* in accordance with the procedures set forth in 12 CFR part 1204.

RECORD ACCESS PROCEDURES:

Direct requests for access to a record to the Privacy Act Officer, Federal Housing Finance Agency, 1700 G Street, NW., Washington, DC 20052, or *privacy@fhfa.gov* in accordance with the procedures set forth in 12 CFR part 1204.

CONTESTING RECORD PROCEDURES:

Direct requests to contest or appeal an adverse determination for a record to the Privacy Act Appeals Officer, Federal Housing Finance Agency, 1700 G Street, NW., Washington, DC 20552 in accordance with the procedures set forth in 12 CFR part 1204.

RECORD SOURCE CATEGORIES:

The information is provided by current and former FHFA employees as well as information retrieved from official FHFA records.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

FHFA–13

SYSTEM NAME:

Freedom of Information Act and Privacy Act Records.

SECURITY CLASSIFICATION:

Unclassified but sensitive.

SYSTEM LOCATIONS:

Office of General Counsel, Federal Housing Finance Agency, 1700 G Street, NW., Washington, DC 20552; 1625 Eye Street, NW., Washington, DC 20006; 1750 Pennsylvania Avenue, NW., Washington, DC 20006; and any alternate work site utilized by employees of the Federal Housing Finance Agency (FHFA) or by individuals assisting such employees.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have submitted requests for information pursuant to the Freedom of Information Act (FOIA); individuals who have submitted requests for records about themselves

under the provisions of the Privacy Act of 1974; individuals filing an administrative appeal of a denial, in whole or part, of any such requests; and individuals filing a civil action in federal court of a denial, in whole or part, of any such requests.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records contain (a) Names, addresses, phone numbers, and other personal information supplied by individuals making written requests pursuant to FOIA; (b)names, addresses, phone numbers, Social Security numbers, and other personal identifying information supplied by individuals making written requests to review or requests for amendment of records to the Privacy Act; (c) correspondence to or from the requester; correspondence to or from an individual writing on the requester's behalf; (d) internal FHFA memoranda; memoranda to or from other federal agencies having a substantial interest in the determination of the request; € responses to requests (including for example acknowledgment letters, fee estimate letters, and final determinations); (f) administrative appeals of denials of a FOIA request; (g) administrative appeals of denials of requests for records or requests for amendment of records made pursuant to the Privacy Act; and (h) and civil actions filed in federal court of a denial, in whole or part, of any such requests. These records may contain personal information retrieved in response to a request. **Note:**FOIA and Privacy Act records may contain inquiries and requests regarding any of FHFA's other systems of records subject to the FOIA and Privacy Act, and information about individuals from any of these other systems may become part of this system of records.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C. 552a), and FHFA implementing regulations, 12 CFR parts 1202 and 1204.

PURPOSE(S):

The records maintained in this system are collected to process requests made under the provisions of FOIA and the Privacy Act. The records are also used by FHFA to prepare reports to the Office of Management and Budget, the Department of Justice, and Congress as required by the FOIA or Privacy Act.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside FHFA as a routine use as follows:

(1) To appropriate federal, state, and local authorities responsible for investigating or prosecuting a violation of, or for enforcing or implementing a statute, rule, regulation, or order issued, when the information indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto;

(2) To a court, magistrate, or other administrative body in the course of presenting evidence, including disclosures to counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal proceedings, when FHFA is a party to the proceeding or has a significant interest in the proceeding, to the extent that the information is determined to be relevant and necessary;

(3) To a congressional office in response to an inquiry made by the congressional office at the request of the individual who is the subject of the record;

(4) To appropriate federal, state, local authorities, and other entities when (a) It is suspected or confirmed that the security or confidentiality of information in the system has been compromised; (b) there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs that rely upon the compromised information; and (c) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(5) To appropriate federal, state, and local authorities in connection with hiring or retaining an individual, conducting a background security or suitability investigation, adjudication of liability, or eligibility for a license, contract, grant, or other benefit;

(6) To appropriate federal, state, and local authorities, agencies, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or corrective actions or grievances or appeals, or if needed in the performance of other authorized duties;

(7) To appropriate federal agencies and other public authorities for use in records management inspections;

(8) To contractor personnel, grantees, volunteers, interns, and others performing or working on a contract, service, grant, cooperative agreement, or project for the Federal Government;

(9) To officials of a labor organization when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions;

(10) To another Federal Government agency having a substantial interest in the determination of the request or for the purpose of consulting with that agency as to the propriety of access or correction of the record in order to complete the processing of requests;

(11) To a third party authorized in writing to receive such information by the individual about whom the information pertains; and

(12) To the Department of the Treasury, federal debt collection centers, other appropriate Federal agencies, and private collection contractors or other third parties authorized by law, for the purpose of collecting or assisting in the collection of delinquent debts owed to FHFA. Disclosure of information contained in these records will be limited to the individual's name, Social Security number, and other information necessary to establish the identity of the individual, and the existence, validity, amount, status and history of the debt.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Pursuant to 5 U.S.C. 552a(b)(12), disclosures may be made from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained in paper form, electronic format, and magnetic disk or tape. Electronic records are stored in computerized databases. Paper and magnetic disk or tape records are stored in locked file rooms or locked file cabinets.

RETRIEVABILITY:

Electronic media and paper format records are indexed and retrieved by the requester's name or by unique log number assigned to the request. Records sometimes are retrieved by reference to the name of the requester's firm, if any, or the subject matter of the request.

SAFEGUARDS:

Records are safeguarded in a secured environment. Buildings where records are stored have security cameras and 24-hour security guard service. Access is limited to those individuals whose official duties require access. Computerized records are safeguarded through use of access codes and other information technology security measures.

RETENTION AND DISPOSAL:

Paper records and electronic media are retained in accordance with National Archives and Records Administration and FHFA Records Retention and Disposition Schedules. Disposal is by shredding or other appropriate disposal systems.

SYSTEM MANAGER(S) AND ADDRESS:

Office of General Counsel, FHFA, 1700 G Street, NW., Washington, DC 20552.

NOTIFICATION PROCEDURE:

Direct inquiries as to whether this system contains a record pertaining to an individual to the Privacy Act Officer, Federal Housing Finance Agency, 1700 G Street, NW., Washington, DC 2052, or *privacy@fhfa.gov* in accordance with the procedures set forth in 12 CFR part 1204.

RECORD ACCESS PROCEDURES:

Direct requests for access to a record to the Privacy Act Officer, Federal Housing Finance Agency, 1700 G Street, NW., Washington, DC 20052, or *privacy@fhfa.gov* in accordance with the procedures set forth in 12 CFR part 1204.

CONTESTING RECORD PROCEDURES:

Direct requests to contest or appeal an adverse determination for a record to the Privacy Act Appeals Officer, Federal Housing Finance Agency, 1700 G Street, NW., Washington, DC 20552 in accordance with the procedures set forth in 12 CFR part 1204.

RECORD SOURCE CATEGORIES:

Requesters and individuals acting on behalf of requesters, FHFA offices and divisions, referrals to or from other Federal agencies having an interest in the request, and employees processing the requests.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

FHFA has or may claim exemptions for several of its other systems of records under 5 U.S.C. 552a (k)(1), (k)(2), and (k)(5) and 12 CFR part 1204. During the processing of a FOIA or Privacy Act request, exempt records from these other systems of records may become part of the case record in this system of records. To the extent that exempt records from other FHFA systems of records are entered or become part of this system, FHFA claims the same exemptions, and any such records compiled in this system of records from any other system of records continues to be subject to any exemption(s) applicable for the records as they have in the primary systems of records of which they are a part.

Dated: May 25, 2011.

Edward J. DeMarco,

Acting Director, Federal Housing Finance Agency.

[FR Doc. 2011–14057 Filed 6–7–11; 8:45 am]

BILLING CODE 8070–01–P

FEDERAL MARITIME COMMISSION

Sunshine Act Meeting

AGENCY HOLDING THE MEETING: Federal Maritime Commission.

TIME AND DATE: June 8, 2011—10 a.m.

PLACE: 800 North Capitol Street, NW., First Floor Hearing Room, Washington, DC.

STATUS: Part of the meeting will be in Open Session and the remainder of the meeting will be in Closed Session.

MATTERS TO BE CONSIDERED:

Open Session

1. Ministry of Transport of the People's Republic of China Request for Adjustment of NVOCC Bond Rider for China Trades—Draft Notice of Inquiry

Closed Session

1. Container Freight Index and Derivatives Working Group—Status Report
2. Staff Briefing on Meetings with Transpacific Stabilization Agreement Representatives and Shipper Representatives

CONTACT PERSON FOR MORE INFORMATION: Karen V. Gregory, Secretary, (202) 523–5725.

Karen V. Gregory,

Secretary.

[FR Doc. 2011–14307 Filed 6–6–11; 4:15 pm]

BILLING CODE 6730–01–P

FEDERAL RESERVE SYSTEM

Consumer Advisory Council; Notice of Meeting of the Consumer Advisory Council

The Consumer Advisory Council will meet on Thursday, June 16, 2011. The meeting, which will be open to public observation, will take place at the Federal Reserve Board's offices in Washington, DC, in Dining Room E on the Terrace Level of the Martin Building. For security purposes, anyone planning to attend the meeting should register no later than Tuesday, June 14, by completing the form found online at: *https://www.federalreserve.gov/secure/forms/cacregistration.cfm*

Attendees must present photo identification to enter the building and should allow sufficient time for security processing.

The meeting will begin at 9 a.m. and is expected to conclude at 12:15 p.m. The Martin Building is located on C Street, NW., between 20th and 21st Streets.

The Council's function is to advise the Board on the exercise of the Board's responsibilities under various consumer financial services laws and on other matters on which the Board seeks its advice. Time permitting, the Council will discuss the following topics:

- **National Mortgage Servicing Standards**

Members will discuss national standards for residential mortgage loan servicing and provide their views on what principles, policies, and procedures such standards should include. They will also address other issues related to current servicing practices.

- **REO Issues**

Members will discuss issues related to the disposition of real estate owned (REO) properties, such as financial institutions' REO management practices, "first look" programs, and the implementation of the regulation providing Community Reinvestment Act consideration for certain neighborhood stabilization activities.

- **Proposed Rules Regarding Ability to Pay for Mortgage Loans**

Members will discuss the Board's proposed rules under Regulation Z (Truth in Lending Act) that would require creditors to determine a consumer's ability to repay a mortgage loan before extending the credit and establish minimum mortgage underwriting standards.

- **Risk Retention Proposal and "Qualified Residential Mortgages"**

Members will provide their views on a proposed rule that would require sponsors of asset-backed securities to retain at least 5 percent of the credit risk of the assets underlying the securities. They will address the proposed