FEDERAL HOUSING FINANCE AGENCY

Information Classification Policy

Approved: Edward J. DeMarco **Date:** 9-27-2012

Edward DeMarco, Acting Director

FEDERAL HOUSING FINANCE AGENCY
INFORMATION CLASSIFICATION POLICY

Title: INFORMATION CLASSIFICATION POLICY

1.0 POLICY

Information created by, obtained by, or communicated to an FHFA employee or FHFA contractor personnel, must be classified and handled appropriately to protect it from loss, theft, unauthorized access or disclosure, compromise, or inappropriate use.

Unauthorized disclosure of FHFA **Non-public** information (including **Restricted** information and information that may become public) by an FHFA employee may result in disciplinary action, up to and including removal from Federal service, or, for FHFA contractor personnel, other appropriate action. Any confirmed or suspected violations of this policy must be reported immediately to FHFA's Chief Information Security Officer and Chief Privacy Officer (CPO).

2.0 SCOPE

This policy applies to all information created by, obtained by, or communicated to an FHFA employee or FHFA contractor personnel, regardless of the medium in which the information resides and regardless of format.

The requirements in this policy are the *minimum* requirements for classifying and handling FHFA information. To the extent that information created by, obtained by, or communicated to an FHFA employee or FHFA contractor personnel is subject to more stringent restrictions, those more stringent restrictions will govern.

3.0 INFORMATION CLASSIFICATION SYSTEM

FHFA's Information Classification System identifies two types of information and establishes the handling requirements for protecting the information.

Division or Office heads are the owners of the information that their office or business unit creates, obtains, or communicates and are responsible for classifying the information into one of the following:

A. **Public -** includes information that has been made available to the general public. This information has no legal restrictions on access or use. Public information may be made available to all FHFA employees, FHFA contractor personnel, or any external party at the discretion of the information owner. **Public** information has a low sensitivity and the risk to FHFA from loss, theft, unauthorized access or disclosure, compromise or inappropriate use is low.

FHFA information is not public until it is made public. ***Until it is made public, it is considered Non-public and must be handled and protected accordingly.***

Public information includes, but is not limited to, information posted to FHFA's public website, such as:

1. FHFA News Releases
2. FHFA House Price Indexes
3. FHFA Regulations published in the *Federal Register*
4. FHFA Annual Report to Congress

B. **Non-public -** includes information that has not been made **public. Non-public** information is information in any medium, whether electronic, hard copy, or unwritten, that FHFA has not made public, that is created by, obtained by, or communicated to an FHFA employee or FHFA contractor personnel, in connection with the performance of official duties, regardless of who is in possession of the information. It does not include information that FHFA has disclosed under the Freedom of Information Act (5 U.S.C. 552; 12 CFR part 1202), or Privacy Act (5 U.S.C. 552a; 12 CFR part 1204). It also does not include specific information or documents that were previously disclosed to the public at large, or information or documents that are customarily furnished to the public at large in the course of the performance of official FHFA duties, including but not limited to: disclosures made by the Director pursuant to the Enterprise Public Use Database Rule (currently located at 24 CFR subpart F, and any FHFA successor rule); the annual report that FHFA submits to Congress pursuant to the Federal Housing Enterprises Safety and Soundness Act of 1992 (12 U.S.C. 4501 et seq.), press releases, FHFA blank forms, and materials published in the *Federal Register*.

Non-public information may be disclosed internally only to FHFA employees and FHFA contractor personnel who have a need to know. **Non-public** information is sensitive and the risk to FHFA from loss, theft, unauthorized access or disclosure, compromise, or inappropriate use is high. Disclosure to parties outside of FHFA must be authorized by the Director or his/her designee.

Non-public information includes, but is not limited to:

1. FHFA reports that have not been approved by the Director for release
2. Unpublished legal opinions
3. Information covered by a non-disclosure agreement
4. Internal memoranda
5. Drafts of all documents

Restricted information is a subcategory of **Non-public** information and is defined as information that is created by, obtained by, or communicated to an FHFA employee or FHFA contractor personnel, that is specifically protected from

disclosure by contractual provision, law, regulation, or privilege. **Restricted** information is subject to more stringent disclosure restrictions than set forth in this policy.

The risk to FHFA from loss, theft, unauthorized access or disclosure, compromise, or inappropriate use of restricted information is extremely high. Accordingly, there may be civil or criminal penalties.

Restricted information includes, but is not limited to:

1. Personally Identifiable Information
2. Trade secrets
3. Proprietary business information
4. Pre-solicitation contract information
5. Information obtained by FHFA that is subject to confidentiality or other specific obligations under a contract or applicable law (e.g., Privacy Act)
6. Continuity of operations information

Non-public and **Restricted** information must be protected from inadvertent loss, theft, unauthorized access or disclosure, compromise, or inappropriate use. **Non-public** and **Restricted** information must be handled, stored, and maintained in a manner to afford adequate protection and prevent unauthorized access. **Non-public** and **Restricted** information may not be posted to any website. Destruction of **Non-public** and **Restricted** information must be done in accordance with FHFA's procedures and all legal requirements.

4.0 FUNCTIONAL RESPONSIBILITIES

A. **Director** (or his/her designee) is responsible for approving the public release of **Non-public** information; granting exceptions to this policy and related procedures; and reviewing and approving agency responses to breaches, actions to mitigate risks, and communications to notify affected individuals and external entities.

B. **Chief Operating Officer** is responsible for providing building security and secured areas where **Non-public** information (including **Restricted** information and information that may become public), can be properly stored and maintained. See FHFA's Facilities Management Policy at http://intranet.fhfa.gov/webfiles/2048/FHFA_Policy_701_%20Facility%20Management_9-22-10.pdf.

Chief Information Officer is responsible for establishing safeguards and IT policies and procedures for handling and protecting **Non-public** information (including **Restricted** information and information that may become public), and complying with requirements to report breaches to the United States Computer Emergency Readiness team. See FHFA's Information Security Technology Policy

at
http://intranet.fhfa.gov/webfiles/2042/FHFA_Policy_209_%20IT%20Security.pdf.

C. **Chief Privacy Officer** is responsible for establishing and implementing policies, procedures, and training for handling and protecting PII; responding to breaches of PII; maintaining reports of the confirmed or suspected breaches of PII; and complying with requirements to report breaches to the United States Computer Emergency Readiness Team. See FHFA's Use and Protection of PII Policy at http://intranet.fhfa.gov/webfiles/2006/FHFA_Policy_301_Use%20and%20Protection%20of%20PII.pdf.

D. **Chief Information Security Officer** is responsible for implementing information security policies and procedures for handling and protecting **Non-public** information (including **Restricted** information and information that may become public); providing information security guidance and training; responding to breaches; maintaining reports of the confirmed or suspected breaches, threats, and malfunctions that may have a security impact on information created or received by FHFA; and complying with requirements to report breaches to the United States Computer Emergency Readiness Team.

E. **General Counsel** is responsible for providing legal advice and counsel on the release of **Non-public** information (including **Restricted** information and information that may become public), to outside parties.

F. **Division and Office Heads** are the owners of the information their division or office creates, obtains, or communicates. They are responsible for identifying the positions in the organization that need access to **Non-public** information (including **Restricted** information and information that may become public); ensuring their staff are trained to appropriately handle and protect **Non-public** information (including **Restricted** information and information that may become public), according to policies, procedures, and legal requirements; designating the secured areas where **Non-public** (including **Restricted** information and information that may become public), must be stored; working with OTIM, OBFM, OHRM, and OGC to create a secure work environment and protect all **Non-public** information (including **Restricted** information and information that may become public); and immediately reporting all confirmed or suspected security breaches.

G. **Managers** and **Supervisors** are responsible for ensuring FHFA employees are trained and aware of their responsibilities for appropriately handling and protecting **Non-public** information (including **Restricted** information and information that may become public), from unauthorized disclosure according to FHFA policies and procedures and immediately reporting all confirmed or suspected security breaches.

H. **Contracting Officer Representatives** are responsible for ensuring FHFA contractor personnel are trained and aware of their responsibilities for appropriately

handling and protecting **Non-public** information (including **Restricted** information and information that may become public), from unauthorized disclosure according to FHFA policies and procedures and immediately reporting all confirmed for suspected security breaches.

I. **All FHFA Employees and FHFA Contractor Personnel** are responsible for following all policies and procedures for handling and protecting **Non-public** information (including **Restricted** information and information that may become public); maintaining awareness at all times of what **Non-public** information (including **Restricted** information and information that may become public), that is on their desk, in their office, and on their laptop; and immediately reporting all confirmed or suspected security breaches.

All FHFA employees and FHFA contractor personnel are required to immediately report any confirmed or suspected breaches to the FHFA Help Desk at (202)649-3990 during regular business hours (7:00 a.m. – 7:00 p.m.) or by email to HelpDesk@fhfa.gov and by email to FHFA Information Security at !OTIMSecurityTeam@fhfa.gov.

All FHFA employees and FHFA contractor personnel are required to immediately report any confirmed or suspected breaches of PII to FHFA's Chief Privacy Officer (CPO) at Privacy@fhfa.gov See FHFA's Breach Notification Policy and Plan at: http://intranet.fhfa.gov/webfiles/2164/FHFA_Policy_601__Breach_Notification_Policy and_Plan.pdf.

5.0 DEFINITIONS

A. **Disclosure** means release of information to persons or entities outside of FHFA.

B. **FHFA employee** means any current or former employee or detailee of FHFA, including any current or former employee within the Office of the Inspector General.

C. **Personally Identifiable Information** means information that can be used to distinguish or trace an individual's identity, such as name, home address, telephone number, social security number, or biometric records, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date of birth or mother's maiden name.

6.0 AUTHORITIES AND REFERENCES

A. Section 208 and Title III, Federal Information Security Management Act of 2002, the E-Government Act of 2002, Public Law 107-347.

B. Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

C. FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

D. Federal Records Act of 1950

E. Freedom of Information Act, 5 U.S.C. 552

F. NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009

G. NIST Special Publication 800-60 Volume 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004

H. NIST Special Publication 800-60, Volume 2, Revision 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008

I. Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*, December 21, 2004

J. OMB Circular A-130, Appendix III *Security of Federal Automated Information Resources*, February 8, 1996

K. OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006

L. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006

M. OMB Memorandum M-07-16, *Safeguarding Against and Responding to Breach of Personally Identifiable Information*, May 2007

N. Privacy Act of 1974, as amended, 5 U.S.C. 552a

7.0 RECORDS RETENTION

Agency records that result from this policy will be retained in accordance with the *FHFA Comprehensive Records Retention Schedule.*