FEDERAL HOUSING FINANCE AGENCY (FHFA)

Breach Notification Policy and Plan

Approved: James B. Lockhart III **Date:** 7/15/09
James B. Lockhart III, Director

TABLE OF CONTENTS

I. PURPOSE:

This establishes the Federal Housing Finance Agency's (FHFA) policy and plan (Policy) to determine what actions must be taken in the event that personally identifiable information (PII) maintained by the FHFA is either lost, stolen or otherwise compromised.

II. SCOPE:

This Policy applies to all FHFA employees and contractors. The Policy covers information in electronic and paper format that is created, collected, or maintained as part of official agency responsibilities.

III. POLICY:

A. Safeguarding Information. Employees and contractors must be knowledgeable about the information in their possession in both electronic and paper formats. Individuals are responsible for safeguarding PII by maintaining appropriate controls (e.g. locking documents in secure file drawers when not in use) at all times.

B. Reporting of Suspected or Confirmed Breaches. In the event an employee or contractor suspects or confirms a breach of PII, the employee or contractor must contact the FHFA Chief Privacy Officer (CPO) immediately.

1. The employee or contractor must provide as much information as possible to the CPO; such as:

   a. Nature of the breach (e.g., lost files, stolen IT equipment, hacked computer access);

   b. Information that was involved in the breach;

   c. Date, time, and location;

   d. Affected individuals; and

   e. Any other pertinent information.

2. The CPO and the Chief Information Officer (CIO) will coordinate actions to appropriately address incidents involving electronic data, systems, and/or devices.

3. Breaches involving PII must be reported to the United States Computer Readiness Team (US-CERT) according to OMB Memorandum 06-19. US-

CERT provides response support and defense against cyber attacks for the Federal Civil Executive Branch. US-CERT is operated by the Cyber Security Division within the Department of Homeland Security. The CPO and the CIO will coordinate in order to properly report incidents to the US-CERT.

C. Initial Assessment. Upon receiving a report of a confirmed or suspected breach, the CPO will assess the incident to determine if a breach has actually occurred and an appropriate course of action. At a minimum, the CPO will do the following:

1. Determine if immediate notification of law enforcement officials is required to secure the safety of FHFA employees, contractors, property or data and coordinate law enforcement notification with the Inspector General, as appropriate.

2. Assess the information reported, consider the type of PII involved (e.g., names, addresses, social security numbers, etc.) and the context of the information (e.g., documents included emergency contact information for Fannie Mae employees) to determine the appropriate action.

3. The CPO's initial assessment will have three possible outcomes:

   a. **Breach of PII has not occurred.** If the incident did not involve FHFA PII, the CPO will document the determination. If the breach involved sensitive agency information (but not PII), the CPO will notify the appropriate Deputy Director who is the owner of the information. For example, the Deputy Director for Enterprise Regulations will be notified if information about Fannie Mae or Freddie Mac was involved in the breach.

   b. **Breach involves low risk PII.** The CPO will assess if the PII is normally publicly available (e.g., name, phone number, address) and identify possible contextual issues of the information involved in the breach. If no further action is required to address the risks to the agency or affected individuals, the CPO will notify US-CERT (as required) and brief the Director.

   c. **Proceed with agency response.** If the CPO determines that the breach may require external notification(s) and further actions are required to address the risks for the agency or affected individuals, the CPO will notify US-CERT (as required), brief the Director, and activate the Core Response Team (CRT).

D. Core Response Team (CRT). The CRT is a group of senior agency officials who are brought together to address suspected or confirmed breaches of PII. The purpose of the CRT is to investigate, assess, report, and tailor the agency's response to suspected or confirmed breaches involving PII. The CRT will be led by the CPO and will include the

Sr. Deputy Director/COO, CIO, the General Counsel, Deputy Director for Enterprise Regulation, Deputy Director for FHLBank Regulation, and the Associate Director for External Relations. Members must send a designee if they are unavailable to attend the CRT meetings.

E. Risk Assessment. The CRT will complete a risk assessment to determine the risk of harm caused by the breach and determine whether and to what extent internal or external notifications are required. The risk assessment must consider the following factors:

1. Nature of the Data Elements Breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. Special consideration should be given to PII that can be used to steal an individual's identity.

2. Number of Individuals Affected. The number of individuals affected by the breach may impact the method of notification but should not determine if notification is required.

3. Likelihood the Information is Accessible and Usable. The likelihood that PII will be or has been used by unauthorized individuals will be a factor in the decision to provide notification. The risk assessment must consider any safeguards in place to protect the data, such as, data encryption of hard drives and mobile devices.

4. Likelihood the Breach May Lead to Harm. The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of information involved in the incident.

5. Ability of the Agency to Mitigate the Risk of Harm. The ability to mitigate risk and monitor for misuse and suspicious behavior will impact the external parties notified of the breach.

F. Action Planning. Once a risk assessment is completed, the CRT will develop a mitigation plan and notification plan to respond to the breach. The plans will be submitted to the Director for review and approval. Upon approval by the Director, the CPO will oversee the execution of the plans and will provide updates to the Director.

1. Mitigation Plan. The CRT will develop a list of mitigation actions to be taken to address risks as result of the breach. The mitigation plan must include plans

for affected individuals, services offered by FHFA (e.g., credit monitoring services), projected costs, and estimated timelines. The CPO will delegate mitigation actions to responsible parties but will be retain overall responsibility for monitoring the completion of the mitigation actions as identified in the mitigation plan.

2. Notification Plan. The CRT will develop a formal notification plan to manage communications between the affected individuals and external stakeholders. The notification plan must address who will receive notifications, who will communicate the notification, the overall message (e.g., what happened, what data was breached, method(s) of notification), and actions the agency will take or has taken to mitigate the risks for affected individuals. In addition, the notification plan must comply with the guidelines set forth in OMB Memorandum M-07-16, Attachment 3, Section B.

G. Post Incident Review. A post incident review will be conducted to identify the root cause(s), analyze the agency's response, and identify improvements to the privacy safeguards. The post incident review will include the CRT and senior management from the FHFA Office(s) involved in the breach. The CPO will designate a senior agency official who was not involved in the breach to lead the post-incident review.

H. Consequences. Failure to comply with this Policy may be considered a violation and subject to disciplinary action. Violations include willful or negligent actions such as the loss of information, unauthorized disclosure, unauthorized access to information, or failure to report breaches. Violation of this Policy may result in disciplinary action up to and including termination and removal from the Federal service. Disciplinary action will consider the specific facts of the violation such as the individual's level of responsibility, the type of information involved, and the employee's intent or negligence.

IV. DEFINITIONS:

- **Access** – Access means the ability or opportunity to gain knowledge of PII.

- **Breach** – The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

- **Incident** – A violation or imminent threat of a violation of security policies, acceptable use policies or standard security practices. An incident may include (but is not limited to) attempts to gain unauthorized access to an agency facility, equipment, network, system or data; unwanted disruption of service; the unauthorized use of a system; and/or changes to

system hardware, firmware, or software without the agency's knowledge, instruction, or consent.

- **Personally Identifiable Information (PII)** – Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

- **Sensitive Information** – Proprietary, legal, financial, and managerial data about FHFA, FHFA employees, or the Regulated Entities.

V. FUNCTIONAL RESPONSIBILITIES:

- **Director** is responsible for reviewing and approving this Policy and agency responses to PII breaches including agency actions to mitigate risks and agency communications to notify affected individuals and external entities.

- **Chief Privacy Officer (CPO)** is responsible for implementing this Policy and periodically evaluating this Policy to ensure agency-wide adherence and effectiveness and that it reflects the agency's needs.

- **Chief Information Officer (CIO)** is responsible for establishing safeguards and IT policies to protect FHFA's hardware, network, systems, and data.

- **General Counsel** is responsible for providing legal advice and counsel to the CPO, CRT and Director.

- **Associate Director of External Relations** is responsible for providing advice and guidance to the CRT and the Director on the communications with external entities and individuals affected by a breach.

- **Deputy Directors** are responsible for establishing safeguards for processes and procedures within their area of responsibility.

- **Managers** are responsible for supervising and instructing assigned employees and contractors to maintain adequate safeguards to protect PII and sensitive information.

- **Employees and contractors** are responsible for reporting breaches involving PII and maintaining appropriate safeguards to protect PII and sensitive information according to FHFA policies, procedures, guidance, and training.

VI. TYPES OF RECORDS CREATED:

Records created will include documents used to address the breach, such as risk assessments, mitigation plans, and notification plans. The records will be maintained in accordance with FHFA records management policy, procedures, and disposition authorities including applicable NARA General Records Schedule items.

VII. AUTHORITY AND REFERENCES:

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

B. Federal Information Security Management Act of 2002

C. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

D. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

E. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002