OFHEO

Director's Advisory

Policy Guidance

Issuance Date: December 19, 2001 Doc. #: PG-01-002

Subject: Safety and Soundness Standards for Information

To: Chief Executive Officers of Fannie Mae and Freddie Mac
OFHEO Deputy Director and Associate Directors

Table of Contents

Subpart A – Introduction

The Policy Guidance on Safety and Soundness Standards for Information sets forth standards pursuant to section 1313 of the Federal Housing Enterprise Safety and Soundness Act (12 U.S.C. 4513). The Guidance addresses standards for developing and implementing

administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of information.

(1) Scope.

The Guidance applies to information maintained by or on behalf of the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac) (collectively, the Enterprises).

(2) Preservation of Existing Authority.

Nothing in the Guidance in any way limits the authority of OFHEO to otherwise address unsafe or unsound conditions or practices or violations of applicable law, regulation or supervisory order. Action referencing the Policy Guidance may be taken separate from, in conjunction with or in addition to any other enforcement action available to OFHEO. Compliance with the Policy Guidance in general would not preclude a finding by the agency that an Enterprise is otherwise engaged in a specific unsafe or unsound practice or is in an unsafe or unsound condition, or requiring corrective or remedial action with regard to such practice or condition. That is, supervisory action is not precluded against an Enterprise that has not been cited for a deficiency under the Policy Guidance. Conversely, an Enterprise's failure to comply with one of the supervisory requirements set forth in the Policy Guidance may not warrant a formal supervisory response from OFHEO, if the agency determines the matter may be otherwise addressed in a satisfactory manner. For example, OFHEO may require the submission of a plan to achieve compliance with the particular requirement or standard without taking any other enforcement action.

(3) Definitions.

For purposes of the Guidance, the following definitions apply:

(a) Information means any record of an Enterprise, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of an Enterprise;

(b) Information security program means the administrative, technical, or physical safeguards used by an Enterprise to access, collect, process, store, use, transmit, dispose of, or otherwise handle information;

(c) Information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of information;

(d) Service provider means any person or entity, including any third party vendor, that maintains, processes or otherwise is permitted access to information through its provision of services directly or indirectly to an Enterprise.

Subpart B – Safety and Soundness Standards for Information

(4) Information Security Program.

Each Enterprise shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the nature and scope of its activities. While all parts of the Enterprise are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

(5) Objectives.

An Enterprise's information security program shall be designed to:

(a) Ensure the security and confidentiality of information;

(b) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(c) Protect against unauthorized access to or use of such information.

Subpart C – Development and Implementation of Information Security Program

(6) Involve the Board of Directors.

The board of directors or an appropriate committee of the board of each Enterprise shall:

(a) Approve the Enterprise's written information security program; and

(b) Oversee the development, implementation, and maintenance of the Enterprise's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

(7) Assess Risk.

Each Enterprise shall:

(a) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems;

(b) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of nonpublic information; and

(c) Assess the sufficiency of policies, procedures, information systems, and other arrangements in place to control risks.

(8) Manage and Control Risk.

Each Enterprise shall:

(a) Design its information security program to manage and control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the Enterprise's activities. Each Enterprise should consider whether the following security measures are appropriate for the Enterprise and, if so, adopt those measures the Enterprise concludes are appropriate:

1. Access controls over information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing information to unauthorized individuals who may seek to obtain this information through fraudulent means;

2. Access restrictions at physical locations containing information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

3. Encryption of electronic information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

4. Procedures designed to ensure that information system modifications are consistent with the Enterprise's information security program;

5. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to information;

6. Monitoring systems and procedures to detect actual and attempted attacks on or intrusion into information systems;

7. Response programs that specify actions to be taken when the Enterprise suspects or detects that unauthorized individuals have gained access to information systems, including appropriate reports to regulatory and law enforcement agencies; and

8. Measures to protect against destruction, loss or damage of information due to potential environmental hazards, such as fire and water damage or technological failures.

(b) Train staff to implement the Enterprise's information security program; and

(c) Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the Enterprise's risk assessment. Tests should be conducted or reviewed by independent third parties or staff that are independent of those that develop or maintain the security programs.

(9) Oversee Service Provider Arrangements.

Each Enterprise shall:

(a) Exercise appropriate due diligence in selecting its service providers;

(b) Require its service providers by contract to implement appropriate measures designed to meet the objectives of the Guidance; and

(c) Where indicated by the Enterprise's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by section 9(b). As part of this monitoring, an Enterprise should review audits, summaries of test results, or other equivalent evaluations of its service providers.

(10) Adjust the Program.

Each Enterprise shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its information, internal or external threats to information, and the Enterprise's own changing business arrangements, such as acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(11) Report to the Board.

Each Enterprise shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the Enterprise's compliance with the Guidance. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

(12) Implementation.

(a) Each Enterprise should implement an information security program pursuant to the Guidance.

(b) Until January 1, 2004, a contract that an Enterprise has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section 9, even if the contract does not include a requirement that the servicer maintain the security and confidentiality of information, as long as the Enterprise entered into the contract on or before the effective date.

Dated: _____

_____

Armando Falcon, Jr.
Director,
Office of Federal Housing Enterprise Oversight.