



governmentattic.org

"Rummaging in the government's attic"

Description of document: Federal Housing Finance Agency (FHFA) Facilities Management Policy, Information Security Technology Policy, 2010 and Policy and Procedures List, 2017

Requested date: 24-January-2017

Released date: 07-February-2017

Posted date: 29-May-2017

Included records: Facilities Management Policy (Policy 701), 2010 starts PDF page 4
Information Security Technology Policy (Policy 209), 2010 starts PDF page 15
Policy and Procedures List, PDF page 24

Source of document: FOIA Request
400 7th Street, SW
8th Floor
Washington, D.C. 20219
Fax: 202-649-1073
FHFA Headquarters - foia@fhfa.gov

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

From: Easter, Stacy <Stacy.Easter@fhfa.gov>
Sent: Tue, Feb 7, 2017 12:21 pm
Subject: FHFA FOIA No. 2017-FOIA-025 February 7, 2017

Re: FHFA FOIA No. 2017-FOIA-025

This letter is in response to your Freedom of Information Act (FOIA) request, dated January 24, 2017. Your request was received in the Federal Housing Finance Agency's (FHFA) FOIA office on January 25, 2017, and assigned FHFA FOIA request number 2017-FOIA-025. Your request was processed in accordance with the FOIA (5 U.S.C. § 552) and FHFA's FOIA regulation (12 CFR Part 1202).

You requested the following:

"Pursuant to the provisions of FOIA, I request a digital/electronic copy of the: 1. FHFA Facilities Management Policy (Policy 701) 2. FHFA Information Security Technology Policy (Policy 209) 3. FHFA Use and Protection of PII Policy (Policy 301) 4. FHFA Breach Notification Policy (Policy 601) 5. A copy of the listing of FHFA Numbered Policies of the type indicated above, from the FHFA employee Intranet site."

A search of FHFA files and records located documents responsive to your request. The FHFA has determined that the documents are releasable in their entirety. See below:

1. FHFA Facilities Management Policy (Policy 701) – attached
2. FHFA Information Security Technology Policy (Policy 209) – attached
3. FHFA Use and Protection of PII Policy (Policy 301) -
https://www.fhfa.gov/AboutUs/Policies/Documents/FHFA_Policy_301_Use-and-Protection-of-PII.pdf
4. FHFA Breach Notification Policy (Policy 601) -
https://www.fhfa.gov/AboutUs/Policies/Documents/FHFA_Policy_601__Breach_Notification_Policy_and_Plan_N508.pdf
5. FHFA Policy List - Attached

Your FOIA request is releasable to the public under subsequent FOIA requests. In responding to these requests, FHFA does not release personal information, such as home or email addresses and home or mobile telephone numbers which are protected from disclosure under FOIA Exemption 6 (5 U.S.C. § 552(b)(6)).

There are no fees associated with processing this request.

If you have any questions regarding the processing of your request, please contact me directly at stacy.easter@fhfa.gov or 202-649-3067 or at foia@fhfa.gov.

Additionally, you may seek dispute resolution services from the Office of Government Information Services (OGIS) at the National Archives and Records Administration. OGIS can be reached at 8601 Adelphi Road – OGIS, College Park, Maryland 20740-6001; by email at ogis@nara.gov; by telephone at 202-741-5770 or toll free at 1-877-684-6448; or by facsimile at 202-741-5769.

Sincerely,

Stacy J. Easter
Freedom of Information Act/Privacy Officer
FOIA Public Liaison
Federal Housing Finance Agency
400 7th Street, SW | Washington, DC 20219
Office: 202-649-3067|Cell: 202-604-1024|Fax: 202-649-4067

Confidentiality Notice: The information contained in this e-mail and any attachments may be confidential or privileged under applicable law, or otherwise may be protected from disclosure to anyone other than the intended recipient(s). Any use, distribution, or copying of this e-mail, including any of its contents or attachments by any person other than the intended recipient, or for any purpose other than its intended use, is strictly prohibited. If you believe you have received this e-mail in error: permanently delete the e-mail and any attachments, and do not save, copy, disclose, or rely on any part of the information contained in this e-mail or its attachments. Please call 202-649-3800 if you have questions.

FEDERAL HOUSING FINANCE AGENCY

FACILITY MANAGEMENT POLICY



Approved: Edward J. DeMarco Date: 9-26-2010
Edward DeMarco, Acting Director

Title: Facility Management Policy

TABLE OF CONTENTS

SECTION 1.0	PURPOSE.....	3
SECTION 2.0	SCOPE	3
SECTION 3.0	AUTHORITY/REFERENCES	3
SECTION 4.0	POLICY	3
SECTION 5.0	FUNCTIONAL RESPONSIBILITIES.....	6
SECTION 6.0	RECORDS RETENTION.....	7

ATTACHMENT A: Administrative Guide for Physical Security

Title: Facility Management Policy

- 1.0 PURPOSE:** To establish Federal Housing Finance Agency (FHFA) policy for managing facilities including physical security, maintenance and repair, and safety.
- 2.0 SCOPE:** This policy covers facilities leased, owned or occupied by FHFA, and applies to FHFA employees, contractors, and visitors to FHFA facilities. It will be administered without regard to race, color, gender, religion, national origin, age, sexual orientation, status as a parent, political affiliation or handicapping condition.
- 3.0 AUTHORITY/REFERENCES:**
- A. Federal Information Security Management Act (FISMA) of 2002, Title III of the E-Government Act of 2002, Public Law 107-347
 - B. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
 - C. Occupational Safety and Health Act of 1970, 29 U.S.C. § 651 et seq.
 - D. Americans with Disabilities Act of 1990, as amended, 42 U.S.C. § 12101 et seq.
 - E. Rehabilitation Act of 1973, 29 U.S.C. § 791 et seq.
- 4.0 POLICY:** FHFA policy is to provide safe and secure, well maintained, and environmentally friendly facilities.
- A. **Physical Security.** FHFA is committed to protecting its facilities, employees, contractors, visitors, assets, information, and resources.
 - 1) All FHFA facilities that permanently house FHFA staff must have:
 - a) On-site security guards, and
 - b) An electronic access system that requires the use of electronic access cards.
 - 2) All FHFA employees, contractors, and visitors to FHFA facilities must be issued a photo identification badge or a visitor badge, which must be clearly displayed at all times while inside the facility.
 - 3) All visitors to FHFA facilities must follow access control procedures to enter the FHFA facility and must be escorted by an FHFA employee at all times while they are in an FHFA facility. FHFA may bar entry or remove any visitor, contractor or

Title: Facility Management Policy

employee to an FHFA facility if the person fails to comply with these or other requirements.

- 4) By entering a FHFA facility, employees, contractors, and visitors implicitly consent to having packages, briefcases, purses, and any other containers in their immediate possession inspected at any time.
- 5) FHFA will provide key or combination locks or other security devices for offices and work spaces, as appropriate.
- 6) Employees, contractors, and visitors may keep personal items in their offices and work spaces; however, FHFA is not responsible for personal items that are lost, stolen or damaged while in a FHFA facility.
- 7) Employees, contractors, and visitors are prohibited from bringing or keeping firearms, knives, explosive devices, or any weapon in a FHFA facility.
- 8) Employees and contractors are generally prohibited from bringing friends or family members into an FHFA facility except for a short visit. Visitors are not permitted to bring friends or family members into an FHFA facility.
- 9) Except where there is a day care center onsite, FHFA facilities may not be used as a substitute for day care.

See Attachment A –Physical Security Guide for specific physical security procedures.

B. Maintenance and Repairs. FHFA is committed to maintaining facilities that function properly and efficiently.

- 1) Maintenance and repairs are managed by the FHFA Facilities Management Office (FMO) which coordinates with building management and vendors to ensure that maintenance and repairs are completed in a timely and satisfactory manner.
- 2) FMO coordinates with building management and cleaning service providers as necessary to ensure that cleaning services are completed in a timely and satisfactory manner.
- 3) Employees and contractors must follow FHFA facility recycling requirements.
- 4) FHFA provides employees and contractors with furniture, fixtures and equipment (FF&E) for use in FHFA facilities. FMO manages maintenance and repair

Title: Facility Management Policy

requests, Division or Office Directors must approve requests for additional or replacement items before requests are submitted to FMO.

- 5) FHFA employees and contractors must maintain their offices and work spaces in a clean and safe manner. FHFA may direct employees and contractors to remove or take down personal or other items if they present a safety or health hazard, are inappropriate or offensive to others, or violate law (e.g., the Hatch Act), regulation, or FHFA policy.

C. Safety. FHFA is committed to protecting employees, contractors, and visitors while in FHFA facilities.

- 1) FHFA facilities will maintain occupant emergency plans and procedures.
- 2) FHFA will comply with applicable health and safety laws, regulations and standards, such as those issued by the Occupational Safety & Health Administration. FMO will monitor and inspect FHFA facilities to oversee compliance, and to address existing or potential issues. This includes procuring, stocking, maintaining, inspecting, and testing supplies, equipment, and facility signage (e.g., first aid kits, automated external defibrillator units, emergency exit signs).

D. Space Utilization. FHFA will provide employees and contractors with work space necessary to perform their official duties.

- 1) FMO is responsible for assigning work space in FHFA facilities in consultation with the relevant division or office. To the extent practicable, FMO will assign work space according to the requirements of the individual's duties. Individuals will be located near their assigned division and office to the greatest extent practicable. FHFA space is managed centrally and is not permanently assigned to any office or division
- 2) New employees and contractors will be assigned a work space after FMO receives confirmation from the Office of Human Resources Management (OHRM) that the employee or contractor is eligible to have access to FHFA facilities.
- 3) Any changes to the facility, work space, and/or work space assignments must be approved in advance by the Deputy Chief Operating Officer (DCOO).

Title: Facility Management Policy

5.0 FUNCTIONAL RESPONSIBILITIES:

- A. **Deputy Chief Operating Officer** is responsible for the development, oversight, and management of FHFA's facilities and the approval of space assignments, alterations and office moves.
- B. **Facilities Management Office** is responsible for implementing this policy, establishing facility management procedures, and managing the day-to-day operations of FHFA's facilities.
- C. **Office of Technology and Information Management** is responsible for identifying special building requirements for housing OTIM equipment (server rooms, electrical and air conditioning, authorizing access to sensitive areas) and coordinating the set up of computer equipment in FHFA facilities.
- D. **Office of Human Resources Management** is responsible for notifying FMO when employees or contractors begin working at FHFA, when they have been cleared for facility access, and when they permanently leave FHFA.
- E. **Equal Employment Opportunity Director** is responsible for coordinating and approving, in consultation with the Office of General Counsel and OHRM, employee requests for reasonable accommodation.
- F. **Division Deputy Directors and Office Directors** are responsible for approving FF&E requests, space requests, space alterations and office moves from subordinate staff prior to submitting to the DCOO.
- G. **Employees and Contractors** are responsible for complying with this policy and administrative guidance and for reporting any building, safety, physical security or other facility matters to FMO.
- H. **Visitors** are responsible for complying with this policy where it relates to them.

6.0 RECORDS RETENTION

Records will be maintained in accordance with FHFA records management policy, and applicable NARA General Records Schedule items.

ATTACHMENT A



Administrative Guide for Physical Security

The Administrative Guide for Physical Security (Guide) sets forth the procedures for maintaining physical security at and access control to FHFA's facilities. This Guide applies to all FHFA occupied facilities, and to all FHFA employees, contractors and visitors to FHFA facilities.

A. Security

1. All facilities that permanently house FHFA staff must have on-site security guard services.
2. FHFA facilities must be equipped with electronic access systems.
 - a. Electronic access is required for external doors and certain sensitive areas (e.g., server rooms and OHRM file rooms). All employees and contractors are required to use an electronic access card to enter FHFA facilities and sensitive areas in FHFA facilities.
 - b. Access to sensitive areas within a facility is restricted to individuals who require access to perform their official duties.
 - c. Contractors will receive electronic access cards, only if they are expected to be at an FHFA facility for 31 or more consecutive calendar days. Contractors who are not issued an electronic access cards must be treated as visitors to FHFA facilities.

B. Visitor Control

1. All visitors must sign in when entering a FHFA facility.

2. Security guard personnel are responsible for issuing and collecting visitor passes and executing post orders related to visitor access.
3. All visitors must be met by a FHFA employee at the facility guard desk and be escorted by a FHFA employee at all times while in a FHFA facility. This requirement to escort a visitor applies to anyone who is not issued a photo identification badge or an electronic access card, and includes former employees and contractors.
4. FHFA employees are responsible for notifying the applicable security desk that visitors are expected and the approximate time of arrival.
5. All visitors must display a visitor identification badge at all times while in a FHFA facility. The visitor must be escorted out of the building by a FHFA employee.

C. Access Cards, Key Fobs, Photo Identification Badges, and Keys

1. Issuance: The following procedures must be followed when issuing access cards, key fobs, photo identification badges, and keys.
 - a. Access cards or key fobs for access to FHFA facilities will be issued upon OHRM notification that an employee or contractor has been cleared for unescorted access to a FHFA facility and FHFA OTIM systems.
 - i. FMO will enroll the individual into the physical access control system and issue the electronic access card and/or key fob.
 - ii. Employees and contractors will be granted general facility access but will not receive access to sensitive areas in an FHFA facility unless approved by the appropriate Office Director.
 - iii. For contractors who are expected to be at FHFA for fewer than six consecutive months, or on a less than full time basis, access will be given only to the primary building in which they are located, unless access to other buildings is approved by the appropriate Office Director. Access will be granted as follows:
 - a. For G Street, access will be granted to the entrance and exit doors only on the 3rd and 4th floors.
 - b. For Pennsylvania Avenue, access will be granted to the entrance and exit doors only on the 9th floor.
 - c. For Eye Street, access will be granted only to the 4th floor elevator lobby. Exceptions may be granted for contractors who require a reasonable

accommodation or whose position requires them to move furniture, fixtures or equipment (e.g., IT Help Desk personnel, etc.).

- b. Employees and contractors who are expected to be at FHFA for six or more consecutive months will be issued an HSPD-12 photo identification badge.
 - i. An HSPD-12 photo identification badge will be issued after the individual satisfies HSPD-12 eligibility requirements.
 - ii. Employees and contractors will be issued a temporary photo identification badge until they receive their HSPD-12 identification badge.
 - c. Employees and contractors, who are expected to be at FHFA for fewer than six consecutive months, will be issued a temporary photo identification badge.
 - d. Before receiving a photo identification badge, or access card/key fob, employees must sign a property receipt form for the item received. This form must be retained for record keeping purposes.
2. Deactivation: The following procedures must be followed when an employee or contractor permanently leaves FHFA.
- a. The individual must turn in his/her photo identification badge, electronic access card, key fob, and office key to FMO on the day of departure.
 - b. FMO must deactivate [or ensure that they are deactivated] electronic access cards and key fobs upon receipt from the departing individual.
 - c. If FMO has not collected the individual's electronic access card or key fob by 3:00 PM on the day of departure, FMO must automatically deactivate the electronic access card and/or key fob by 5:00 p.m. of that day.
 - d. FMO must notify the security guards that the departing individual is no longer working at FHFA and that, should they return to FHFA as visitors, they must be signed in and escorted at all times in FHFA facilities.
 - e. If the individual requires access to a FHFA facility after 5:00 p.m. on the day of departure, the individual must be escorted by a supervisor, COTR or another FHFA employee.
3. Temporary access: If an FHFA employee or contractor requests a temporary access card or key fob:

- a. FMO will issue a temporary access card or key fob to the individual with pre-established access privileges. The card will expire on the same day the access card or key fob is issued.
- b. The individual must sign a property receipt form. The form must be retained for record keeping purposes.
- c. The individual must return the access card or key fob to FMO or place it in a secured mailbox (1700 G St. - mail room # 4129 and 1625 Eye St. – copy room # 3043) at the end of the day.

4. Keys

- a. FMO will manage and maintain individual office keys, building master keys and combinations to combination locks.
- b. Individuals issued an individual office key, building master key, or combination to a combination lock must sign a property receipt form which will be retained as a record.
- c. FMO must maintain in a secure location a key and combination control book containing a list of individuals issued keys with property receipt documents, combinations for door locks and correspondence regarding measures employed to safeguard master keys issued to non-FMO staff.

5. Lost, stolen or damaged photo identification badge, access card, key fob or key:

- a. Employees and contractors must immediately inform FMO if their FHFA issued photo identification badge, access card, key fob, or key is lost, stolen or damaged.
- b. FMO must immediately deactivate the access card or key fob upon notification by the employee or contractor.
- c. FMO must issue a replacement access card, key fob, office key, or photo identification badge, whether temporary or HSPD-12, as soon as possible after being informed of the loss, theft, or damage.

D. Access Reconciliations and Reports


- 1. FMO must perform quarterly reviews of all FHFA sensitive area and contractor access logs.
 - a. FMO will require each FHFA division/office with access to sensitive areas (e.g. OTIM or OHRM) to validate access rights for authorized individuals who have been granted access to the sensitive area during the most recent quarter.

- b. FMO will require each COTR responsible for managing contractors to validate access rights granted to contractors during the most recent quarter.
- 2. FMO will create ad hoc reports of access history as needed.

FEDERAL HOUSING FINANCE AGENCY

Information Technology Security Policy



Approved: 
Melvin L. Watt, Director

Date: 8/7/2014

FHFA Information Technology Security Policy Table of Contents

I. Policy	Page 3
II. Scope.....	Page 3
III. Purpose.....	Page 3
IV. Responsibilities.....	Page 3
V. Definitions.....	Page 8
VI. Authorities and References	Page 8
VII. Records Retention.....	Page 9

I. Policy

Federal Housing Finance Agency (FHFA) policy is to protect and secure agency information technology (IT) resources by complying with applicable federal laws, regulations, and guidance on IT security.

In areas where federal guidelines are lacking or still evolving, FHFA will implement IT security policies and procedures based on industry best practices within the IT security community.

This overall FHFA IT Security Policy will be supported by additional formal, documented IT policies specific to various IT security topics, to address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance. Documented IT security procedures are used to facilitate the implementation of FHFA IT security policies.

II. Scope

This Policy applies to FHFA employees, contractors, and service providers who have specialized roles supporting IT systems and must comply with day-to-day requirements of IT security policies (e.g., incident reporting, prompt system upgrades).

Day-to-day user responsibilities for using FHFA IT resources can be found in the [FHFA Information Systems Rules of Behavior](#).

III. Purpose

This document establishes the IT Security Policy (Policy) and standards for the FHFA IT Security Program, hereafter referred to as the FHFA Cybersecurity Program. This Policy implements the requirements specified for all federal agencies in the Federal Information Security Management Act (FISMA) of 2002 and related laws, regulations, and other mandatory guidance and standards related to information security.

The Policy prescribes responsibilities, practices, and conditions that directly or indirectly promote IT security in the development, operation, maintenance, and support of all FHFA IT resources.

The Policy identifies security practices that are appropriate to FHFA's mission, provides cost-effective protection of FHFA's information and information systems, responds to security issues associated with contemporary technologies and risks, and is consistent with current applicable federal security laws, policies, and regulations.

IV. Responsibilities

- A. The Director** of FHFA is responsible for ensuring that FHFA information systems are protected in accordance with applicable laws, regulations, and guidance. To that end, the Director will ensure the Chief Information Officer (CIO), Chief Information

Security Officer (CISO), Program Offices, and System Owners have the support and resources they need to effectively implement IT security throughout FHFA.

- B. The Chief Information Officer**, under the responsibility and authority granted by the Clinger-Cohen Act of 1996 (P.L. 104-106), FISMA, and the Office of Management and Budget (OMB) Memo M-09-02, *Information Technology Management Structure and Governance Framework*, ensures that the FHFA Cybersecurity Program is developed, documented, and implemented to provide security for all FHFA information systems, networks, and data that support FHFA operations.

The CIO is responsible for the overall Cybersecurity Program highlighted in this Policy and will advise the Director of any program level changes. The CIO appoints, in writing, the CISO and reports annually to the Director on the effectiveness of the agency Cybersecurity Program, including progress of any required remedial actions. The CIO is responsible for developing and approving Cybersecurity policies and procedures subordinate to this Policy and may delegate this authority to the Chief Information Security Officer.

- C. The Chief Information Security Officer** manages FHFA's Cybersecurity Program and has the responsibility and authority for carrying out security responsibilities under FISMA. The CISO, with the support of the Office of Technology and Information Management (OTIM) staff, establishes a strong foundation for FHFA IT security by maintaining the FHFA Cybersecurity Program. The CISO interacts with internal and external resources and coordinates cybersecurity compliance across FHFA organizational elements. The CISO is responsible for developing Cybersecurity policies and procedures subordinate to this Policy, and approving those policies if delegated by the CIO. The CISO seeks advice from key stakeholders during policy development and will advise the CIO on program level changes.
- D. The OTIM Chief Technology Officer** is the system owner for the IT infrastructure (e.g., the general support system) that provides shared IT services across FHFA. Following FHFA IT security program policy and guidance, the Chief Technology Officer ensures the implementation of IT security controls to secure FHFA's IT assets.
- E. The OTIM Security Group**, under the management of the FHFA CISO, is responsible for implementing the agency's operational cybersecurity measures and for ensuring the agency's compliance with FISMA requirements. This includes, but is not limited to, the establishment of the agency's information security training and awareness program, the security assessment and authorization of agency information systems, and the management of the agency's cybersecurity incident response program.

Additionally, the OTIM Security Group performs a central Information System Security Officer (ISSO) function for all FHFA information systems, responsible for

- ensuring that management, operational, and technical controls for securing the systems supporting the program offices are in place and effective. The OTIM Security Group acts as the principal point of contact for information system security and is responsible for all security aspects of FHFA information systems from inception through disposal.
- F. Facilities Operations Management (FOM)** is responsible for the physical security of FHFA leased or owned facilities, for issuing badges, and for managing facility access. FOM is also responsible for the physical and environmental security controls that protect FHFA's IT assets.
- G. The Office of Human Resources Management** is responsible for defining position sensitivity levels for government positions and risk levels for contractor positions, for performing security background investigations when necessary, and for providing security related exit procedures when employees and contractors leave FHFA.
- H. The Senior Agency Official for Privacy** is responsible for ensuring that the FHFA remains in compliance with applicable laws and regulations governing privacy.
- I. The Senior Procurement Executive (SPE)** ensures that FHFA contracts for IT systems and services include appropriate IT security clauses as provided by OTIM. OTIM works with the SPE and interested stakeholders (e.g., program office sponsoring the acquisition) and the Office of General Counsel, to develop IT security contract clauses, as appropriate, based on current policies, regulations, and guidance for FHFA IT systems and services.
- J. Contracting Officers (COs)** have authority to enter into, administer, and terminate contracts per their Certificates of Appointment. For contracts supporting IT systems and services, the COs shall ensure that:
1. New contracts include appropriate clauses and other terms and conditions, provided by OTIM, to comply with FHFA IT Security Policy.
 2. New contracts incorporate IT security functional and assurance requirements, provided by OTIM, in accordance with FHFA IT Security Policy.
 3. All contractual IT security terms and conditions comply with FHFA's Acquisition Policy.
 4. Existing contracts may be modified when necessary to include appropriate terms and conditions to enforce FHFA IT security policies (as described above), if such contracts did not originally include such terms and conditions at time of award, and either the contract's requirements have changed subsequent to award to require such terms and conditions, or such terms and conditions should have been included at time of contract award.

- K. Contracting Officer Representatives (CORs)** are FHFA employees with responsibility to monitor contractor employees' compliance with contract terms, including requirements under the Privacy Act and the Rules of Behavior. CORs are responsible for notifying the Contracting Officer and the CISO of any known failures of contractor employees' compliance with this Policy, and for notifying the Help Desk when contractor personnel are terminated, transferred, or no longer need access to an information system or resource. CORs will review the IT security clauses in their contracts and work with their Contracting Officer and the IT Security Group to assess if a modification is appropriate.
- L. The Office of General Counsel** provides legal advice on IT security related matters.
- M. Information Owners** are FHFA employees with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. They are responsible for ensuring that only users with a valid need (i.e., in the performance of their official duties or duties under an authorized contract) are provided access to non-public information, and that they are provided with the lowest level of access to the data (e.g., read only) necessary to perform their job function.
- N. System Owners** are FHFA employees responsible for defining the operating parameters, authorized functions and security requirements of an information system. The system owner may or may not be the information owner of the information processed by the information system. They are responsible for ensuring that only users with a valid need (i.e., in the performance of their official duties or duties under an authorized contract) are provided access to the information system, and that they are provided with the lowest level of access to the data (e.g., read only) necessary to perform their job function.
- O. System Administrators** are responsible for implementing and maintaining technical controls that enforce operational and managerial controls through mechanisms contained in the hardware, software, or firmware components of the information system. System administrators must maintain an environment that creates a strong technical foundation for enforcement of information system security.
- P. The Certification Agent** provides an impartial and unbiased assessment of FHFA information systems independently from the individuals directly responsible for information systems development and day-to-day system operations. The Certification Agent assesses all security documentation for the system and validates that the system has been assessed in accordance with FHFA's security assessment and authorization process.
- Q. The Authorizing Official** is a senior government official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. The CIO is FHFA's authorizing official. Authorizing Officials control personnel, operations, maintenance, and budgets for their systems thereby controlling

the resources necessary to mitigate risks to their information systems. Authorizing Officials may designate a representative to act on their behalf to make certain decisions regarding the planning and resources for security activities, acceptability of security authorization documentation, and the determination of risk to agency operations, agency assets, and individuals. The Authorizing Official may not delegate the security authorization decision and signing of the associated authorization decision letter.

- R. Supervisors** authorize issuance of IT system access for their staff and are directly responsible for notifying System Owners when staff members are terminated, transferred, or no longer need access to a system.
- S. Users** is a broad term used for all personnel that interact with FHFA information system resources either in a support function, by working directly with an information system resource (e.g., system user), or as a recipient of FHFA information (e.g., information user). For the purposes of this document, users include both FHFA employees and contractors who provide services and resources to FHFA. User responsibilities include the following:

 - 1. Comply with FHFA Information Systems Rules of Behavior.
 - 2. Assume accountability for protecting sensitive information, including personally identifiable information, under their control in accordance with this policy.
 - 3. Complete annual IT security awareness training.
 - 4. Attend required role-based security training pertaining to those having a security related role (e.g., system or network administrators).
 - 5. Report information security incidents (e.g., viral infections, malicious code attacks) to the FHFA Help Desk (email: HelpDesk@fhfa.gov) and to the OTIM Security Group (email: OTIMSecurityTeam@fhfa.gov) according to established procedures.
 - 6. Cooperate with the OTIM Security Group in the investigation of security incidents.
 - 7. Cooperate with the OTIM Security Group or other designated FHFA Program Office personnel during security compliance reviews at FHFA Program Office facilities and site surveys at non-FHFA facilities.
 - 8. Understand and comply with FHFA policies, standards, and procedures regarding the protection of sensitive FHFA information assets.
- T. Individuals with Key Contingency Roles**, as defined in systems' contingency plans, must receive training and be prepared to perform the required functions as defined in those plans.

- U. **Service Providers** are contractors that provide IT services, IT systems, and facilities hosting FHFA information. Service providers are responsible for maintaining security controls that are compliant with FHFA security policy and procedures.
- V. **Developers** are responsible for developing, maintaining, and implementing IT systems that comply with FHFA IT security policies and procedures, National Institute of Standards and Technology (NIST) guidance, and federal regulations.

V. Definitions

Authentication – Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Information – Data in electronic form that is generated, classified, collected, processed, disseminated, preserved, and disposed of using FHFA systems as well as hardcopy outputs on FHFA information systems. Examples include documents, emails, and research data (e.g., Excel spreadsheets).

Personally Identifiable Information – 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.

VI. Authority and References

FHFA has established an agency-wide IT security policy based on the following Executive Orders, public laws, and U.S. Government agency policies:

- A. Federal Information Security Management Act (FISMA), Title III of E- Government Act of 2002 (P.L. 107-347), December 2002.
- B. Paperwork Reduction Act of 1995 (P.L. 104-13), May 1995.
- C. Government Paperwork Elimination Act (P.L. 105-277), October 1998.
- D. Privacy Act of 1974, as amended (P.L. 93-579), December 1974.
- E. Clinger-Cohen Act of 1996 (P.L. 104-106), February 1996.
- F. Office of Management and Budget (OMB), Circular No. A-130, Appendix III, Transmittal Memorandum No. 4, *Management of Federal Information Resources*, November 28, 2000.
- G. OMB Memorandum M-09-02, *Information Technology Management Structure and Governance Framework*, October 21, 2008.

- H. OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.
- I. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006.
- J. OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005.
- K. OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003.
- L. OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.
- M. Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- N. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
- O. National Institute of Standards and Technology (NIST) Special Publications (800 Series).
- P. FHFA Information Systems Rules of Behavior, March 2014.

VII. Records Retention

All FHFA IT security policies, procedures and artifacts from IT Security activities such as security assessment and authorizations, vulnerability assessments, risk assessments, audit logging, incident response, etc., are classified as item 5.4 of the FHFA Comprehensive Records Schedule (N1-543-11-1), and shall be retained for seven (7) years after the project/activity is completed.

POLICIES & PROCEDURES

The following policies have been approved for FHFA use:

OFFICE OF THE DIRECTOR	BUDGET & FINANCE	CONGRESSIONAL AFFAIRS & COMMUNICATIONS
FHFA Official Documents Policy (Policy 801) <ul style="list-style-type: none"> FHFA Style Guide (Policy 801-4) Chicago Manual of Style Staff Analysis Template (Policy 801-2) Executive Summary Template (Policy 801-3) Administrative Policy Template (Policy 801-5) Clearance Sheet for Executive Review Template (Form 001d) 	<ul style="list-style-type: none"> Acquisition Policy (Policy 503) Capitalization Policy (Policy 502) Expenditure of Agency Funds for Food, etc. (Policy 505) Property Management Policy (Policy 501) Travel Policy (Policy 506) 	<ul style="list-style-type: none"> Congressional Inquiries Policy (Policy 401) Public Inquiries Policy (Policy 403)
GENERAL COUNSEL	HUMAN RESOURCES	INFORMATION TECHNOLOGY
<ul style="list-style-type: none"> Breach Notification Policy and Plan (Policy 601) Privacy Threshold Analysis and Privacy Impact Assessment Guide Procedures on How and When to Draft a Privacy Act System of Records Notice Use and Protection of Personally Identifiable Information Policy (Policy 301) Freedom of Information Act (FOIA) Procedures - May 2012 Procedures for Monitoring Information Technology Systems that Contain Personally Identifiable Information - August 2015 Federal Housing Finance Agency Privacy Program Plan - August 2015 Guidance on How and When to Respond to a Request for Amendment or Correction of a Record Contained in an FHFA System of Records - April 2014 Guidance on Accounting for Disclosures of Information Contained in an FHFA System of Records - April 2014 Protecting PII: Teleworking or Working Remotely 	<ul style="list-style-type: none"> Absence and Leave Policy (Policy 112) Administrative Grievance Policy (Policy 104) Executive Compensation Policy (Policy 103) Employment and Placement Policy (Policy 118) Awards Policy (Policy 115) Conduct and Discipline Policy (Policy 117) Domestic Violence, Sexual Assault and Stalking Policy (Policy 116) Merit Promotion Plan Policy (Policy 105) Non-Executive Compensation Policy (Policy 102) Performance Management Policy (Policy 101) Premium Pay Policy (Policy 111) Training Policy (Policy 114) Reimbursements and Stipends Policy (Policy 113) Telework Policy (Policy 109) Work Schedule Policy (Policy 110) Duty Station Policy (Policy 119) Reasonable Accommodation Policy and Procedures (Policy 106) 	<ul style="list-style-type: none"> FHFA Comprehensive Records Schedule Records Management Policy (Policy 207) Information System Rules of Behavior (ROB) - September 2016 FHFA Information Technology Security Policy (Policy 209) System Development Lifecycle (SDLC) Policy (Policy 205) System Development Lifecycle (SDLC) Process and Procedures FHFA Information Classification Policy (Policy 221) FHFA Information Classification and Handling Procedures (Relates to Policy 221) FHFA Personally-Owned Device Wireless Network Terms of Use - January 2013
DIVISION OF CONSERVATORSHIP	OPERATIONS	OFFICE OF MINORITY & WOMEN INCLUSION / EEO SERVICES
<ul style="list-style-type: none"> Conservatorship Committee Charter Consumer Communications Procedures (related to Policy 405) External Communications Standards for Enterprises in Conservatorship Procedures for Implementing the Conservatorship Decision Protocols Conservatorship Decision Protocols Policies Related to Consumer Communications (Policy 405) Settlement Policy and Settlement Procedural Guide 	<ul style="list-style-type: none"> Facility Management Policy (Policy 701) Vehicle Use Policy (Policy 702) Parking Policy (Policy 703) Space Management Policy (Policy 704) FHFA Correspondence Processing Policy (Policy 203) Parking Policy Application Instruction Guide (Related to Policy 703) Trakker Procedures (related to Policy 203) 	<ul style="list-style-type: none"> Anti-Harassment Policy, Procedures, and Responsibilities (Policy 802) EEO Anti-Harassment Policy Statement (Related to Policy 802)