FEDERAL HOUSING FINANCE AGENCY

Controlled Unclassified Information Policy

Approved: SANDRA THOMPSON

Digitally signed by SANDRA THOMPSON
Date: 2024.07.10 15:22:28 -04'00'

Sandra L. Thompson, Director

Controlled Unclassified Information Policy

Table of Contents

I. POLICY

The Controlled Unclassified Information (CUI) Policy establishes the principles governing the appropriate designation, management, and protection of all information created by or in the possession of the Federal Housing Finance Agency (FHFA).

II. DEFINITIONS

A. **Breach.** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where a person accesses or potentially accesses CUI that the person is not authorized to access.

B. **Controlled Unclassified Information (CUI).** Information the federal government creates or possesses, or that an entity creates or possesses for or on behalf of the federal government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. The National Archives and Records Administration (NARA) has established an online repository, the CUI Registry,[1] which identifies and describes all CUI as one of two types: CUI Basic and CUI Specified.

1. **CUI Basic.** Underlying authorities for information designated as CUI Basic do not set out specific handling or dissemination controls. CUI Basic information is subject to the uniform safeguarding and dissemination controls that are addressed in FHFA's CUI Procedures. FHFA Non-Public Information, as defined in 12 CFR 1214.1, is a registered CUI category and is designated as CUI Basic.

2. **CUI Specified.** Information designated as CUI Specified is subject to specific handling, marking, and dissemination requirements that differ from and may be more stringent than the uniform set of controls for CUI Basic. The distinction is that the underlying authority spells out specific controls for CUI Specified information.

C. **Confidential Supervisory Information.** As defined in 12 CFR 1214.1, information prepared or received by FHFA that meets all of the following criteria:

1. The information is not a document prepared by a Regulated Entity or the Office of Finance for its own business purposes that is in its possession;

2. The information is exempt from the Freedom of Information Act; and

[1] The CUI Registry is available at https://www.archives.gov/cui/registry/category-list.

3. The information:

a. Consists of reports of examination, inspection and visitation, confidential operating and condition reports, and any information derived from, related to, or contained in such reports, or

b. Is gathered by FHFA in the course of any investigation, suspicious activity report, cease-and-desist order, civil money penalty enforcement order, suspension, removal or prohibition order, or other supervisory or enforcement orders or actions taken under the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, Public Law 102-550, 122 Stat. 2654.

D. CUI Registry. The online repository for all NARA-issued information, guidance, policy, and requirements on handling CUI. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, establishes markings, and includes guidance on handling procedures. The CUI Registry also identifies the laws, regulations, and government-wide policies that contain the specific handling and dissemination controls for CUI Specified information.

E. Decontrol. Decontrol occurs when the Information Owner, in coordination with the Office of General Counsel (OGC), determines that information marked as CUI no longer requires protection as CUI. However, decontrolled CUI may be released to a third party or the public only if authorized in writing by the Director or a delegate.[2]

F. Disclosure/Dissemination. The release or divulgence of information by any FHFA employee or contractor personnel to any person or entities outside of FHFA.

G. FHFA Contractor Personnel. Any current or former contractor or its personnel, including directors, officers, employees, subcontractors, agents, or consultants, to the extent that the protection of CUI or Non-Public Information is addressed in their contract.

H. FHFA Employee. Any person employed by FHFA, including any current or former officer, intern, agent, or detailee of FHFA.

I. FHFA Information. Information created by, obtained by, or communicated to an FHFA employee (or an FHFA contractor or its personnel) in connection with the performance of official duties, regardless of who is in possession of the information.

[,k2] See FHFA Delegations and Designation Orders.

J. **Information Owners.** Division and Office heads are the owners of FHFA Information that their division or office creates or obtains from a third party.

K. **Non-Public Information.** As defined in 12 CFR 1214.1, information that FHFA has not made public that is created by, obtained by, or communicated to an FHFA employee or contractor personnel in connection with the performance of official duties, regardless of who is in possession of the information. This includes Confidential Supervisory Information as defined above. It does not include information or documents that are customarily furnished to the public in the course of the performance of official FHFA duties. It also does not include information or documents that FHFA has disclosed under the Freedom of Information Act or Privacy Act of 1974.

L. **Personally Identifiable Information (PII).** Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII is an example of CUI Specified.

M. **Public Information.** FHFA Information that has been approved for public release and made available to the public. Public Information has no legal restrictions on access or use. Public Information has low sensitivity, and the risk to FHFA from loss, theft, unauthorized access or disclosure, compromise or inappropriate use is negligible.

N. **Regulated Entities.** Federal National Mortgage Association (Fannie Mae) and any affiliate thereof (including Common Securitization Solutions), the Federal Home Loan Mortgage Corporation (Freddie Mac) and any affiliate thereof (including Common Securitization Solutions), and any Federal Home Loan Bank.

O. **Senior Agency Official (SAO) for CUI.** Designated in writing by an agency head and responsible to that agency head for implementation of the CUI Program within that agency. FHFA's Chief Information Officer is designated as the SAO for CUI.

III. SCOPE

This Policy applies to all information created by, obtained by, or communicated to FHFA employees or contractor personnel in connection with the performance of official duties, regardless of the medium in which the information resides. This Policy applies to all FHFA employees and to contractor personnel to the extent specified by their contract.

IV. CONTROLLED UNCLASSIFIED INFORMATION PROGRAM

Executive Order (E.O.) 13556, Controlled Unclassified Information, dated November 4, 2010, designates the National Archives and Records Administration (NARA) to oversee the CUI Program for the executive branch of the federal government. As part of that responsibility, NARA issued 32 CFR Part 2002, Controlled Unclassified Information, effective November 14, 2016, which established a government-wide policy governing the management and oversight of CUI.

A. Categories of Information and CUI Marking

FHFA Information generally falls into one of two categories: Public Information or CUI.

1. **Public Information** is information that has been approved for public release and made available to the public. Public Information has no legal restrictions on access or use. Public Information has low sensitivity, and the risk to FHFA from loss, theft, unauthorized access or disclosure, compromise, or inappropriate use is negligible. No explicit designations or markings are required for Public Information.

2. **CUI** is any information that a federal agency creates or possesses, or that an entity creates or possesses for or on behalf of a federal agency, that is subject to any safeguarding or dissemination controls under federal law, regulation, or governmentwide policy. CUI can in turn be divided into one of two overarching types: **CUI Basic** or **CUI Specified**.

All FHFA Information designated as CUI Basic or CUI Specified must be handled according to controls as defined in 32 CFR Part 2002 and the CUI Registry and must be marked as provided in the CUI Procedures and related training.

B. Safeguarding Measures and Dissemination Controls

Most FHFA Information is CUI and reasonable precautions must be taken to guard against unauthorized disclosure of CUI by properly securing systems, controlling dissemination, and applying CUI markings to documents. In safeguarding CUI, FHFA employees and contractor personnel are required to mark documents appropriately. Detailed instructions for protecting, disseminating, and marking CUI are provided in the CUI Procedures.

1. **Disclosure of CUI** – Except as described below, only the Director or a delegate[3] may authorize the disclosure of CUI to entities or individuals

[3] See FHFA Delegations and Designation Orders.

outside of FHFA. Unauthorized disclosure of CUI 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, including contract termination.[4] Employees or contractor personnel who improperly disclose CUI may also be subject to civil and/or criminal penalties, depending on the nature of the information disclosed.

2. **Disclosure of CUI to other FHFA employees, the Regulated Entities, or the Office of Finance** – Current FHFA employees and contractor personnel may disclose or permit the disclosure of CUI to other FHFA employees or contractor personnel, the Regulated Entities, or the Office of Finance when necessary and appropriate for the performance of their official duties. CUI disclosed to the Regulated Entities, or the Office of Finance must be properly marked to ensure the recipient is aware of the information's status as CUI that requires protection.

3. **Exception for Disclosure of CUI in Court and Administrative Proceedings –** Notwithstanding any other provision in this Policy, employees and contractor personnel, as part of the performance of their official FHFA duties, may disclose CUI to parties, courts, or other adjudicative bodies where the disclosure has been ordered by a court or adjudicative body of competent jurisdiction or is otherwise required and appropriate as part of a proceeding before a court, administrative tribunal or any other adjudicative body. Such adjudicative bodies include, but are not limited to, the Equal Employment Opportunity Commission, the Merit Systems Protection Board, and the Office of Personnel Management (for the purpose of adjudicating retirement applications).

4. **Exception for CUI required to be shared with the National Treasury Employees Union (NTEU)** – Notwithstanding any other provision in this Policy, FHFA's Labor Relations Staff, or other appropriate Office of Human Resources Management or Office of General Counsel (OGC) employees, as part of the performance of their official FHFA duties, may disclose CUI to the NTEU as legally required. FHFA employees who are official NTEU representatives may also disclose CUI while engaged in representative activities.

5. **Safeguarding and Handling CUI** – FHFA employees and contractor personnel are responsible for preventing unauthorized access to or disclosure of CUI in both physical and electronic environments, including while

[4] CUI markings or lack of markings do not determine whether the information may be properly released pursuant to the Freedom of Information Act or the Privacy Act of 1974. Disclosure determinations under the Freedom of Information Act and the Privacy Act are based solely on application of the criteria set forth in those laws.

teleworking, traveling, or working at field locations by securing physical CUI behind at least one locked barrier when not under their direct control.

6. **Decontrolling CUI** – Decontrolling refers to the process by which FHFA determines that FHFA Information designated as CUI no longer requires protection as CUI. The decision to decontrol CUI is made by the Information Owner in consultation with OGC. However, the process of decontrolling CUI affects only the safeguarding required for the decontrolled information not the dissemination of the information. CUI that is decontrolled may be released to a third party or the public only if authorized by the Director or a delegate.

7. **Whistleblowing Activity Not Restricted** – With respect to FHFA employees, nothing in this Policy or any related procedures prohibits or restricts an employee from disclosing to Congress, the Office of Special Counsel, the Inspector General, or any other Agency component responsible for internal investigation or review, any information that relates to any violation of law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or any other whistleblower protection. Pursuant to the Whistleblower Protection Enhancement Act of 2012, as amended, employees are provided the following notice with respect to this Policy: These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General or the Office of Special Counsel of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive Orders and statutory provisions are incorporated into this agreement and are controlling.

C. Training

FHFA employees are required to complete mandatory initial training, as well as mandatory annual training on identifying, protecting, and marking CUI. Contractor personnel shall be required to complete CUI training as specified by their contract.

D. Incident Management and Breach Response

Immediately report suspected or confirmed breaches of CUI to the FHFA Help Desk at HelpDesk@fhfa.gov or (202) 649-3990 during regular business hours between 6:00 a.m. – 7:00 p.m., ET. After regular business hours, during unscheduled office closures, on weekends, and on holidays, immediately report

suspected or confirmed breaches of CUI by calling the FHFA Help Desk.

E. Self-Inspection Program

FHFA will conduct a self-inspection review of its CUI Program on an annual basis. This self-inspection review will incorporate methods to evaluate CUI Program implementation, effectiveness, and measure compliance.

F. Agency Reporting

Annual reports on the status of FHFA's CUI Program implementation, FHFA's self-inspection program, and any additional requested reports will be provided to NARA as required.

V. RESPONSIBILITIES

A. **Director** is responsible for delegating roles and responsibilities for the CUI Program. Except as provided for in this Policy, only the Director or a delegate may authorize the disclosure of CUI to third parties or the public.

B. **Chief Information Officer** is designated as the **SAO for CUI** and is responsible for implementing and overseeing FHFA's CUI Program to include compliance, management, and establishing policies, procedures, and processes for the CUI Program. The SAO for CUI is the primary point of contact for official correspondence, accountability reporting, and other matters of record related to CUI.

C. **General Counsel** is responsible for providing legal advice and counsel on this Policy as well as legal advice relating to the disclosure and decontrol of CUI.

D. **Chief Information Security Officer (CISO)** is responsible for implementing security policies and procedures for handling and protecting CUI; developing any necessary contract clauses and associated prescriptions with respect to information security; providing information security guidance and training; responding to breaches; maintaining reports of confirmed or suspected breaches, threats, and malfunctions that may have a security impact on FHFA Information, including CUI; and complying with requirements to report breaches to the United States Computer Emergency Readiness Team (US-CERT).

E. **Senior Agency Official for Privacy** is responsible for establishing and implementing policies for handling and protecting Personally Identifiable Information (PII); responding to PII breaches; maintaining reports of confirmed or suspected breaches of PII; and complying with requirements to report breaches to the US-CERT.

F. **Records Officer** is designated as the **CUI Program Manager** and serves as the official representative to NARA for CUI-related activities. The CUI Program Manager is responsible for developing and implementing policies and procedures for the CUI Program, providing guidance and training, responding to incidents, reporting on the CUI Program, and working with the CISO to establish safeguards and information technology procedures for handling and protecting CUI. The CUI Program Manager also coordinates FHFA's CUI Self-Inspection Review activities.

G. **Division and Office Heads** are the owners of FHFA Information that their division or office creates, obtains, or communicates. They are responsible for:

1. Complying with FHFA requirements, policies, and procedures for CUI;

2. Identifying individuals/positions on their staff that need access to CUI;

3. Ensuring staff complete any required CUI training;

4. Designating the secured areas where CUI must be stored;

5. Reviewing requests to disseminate CUI to third parties, prior to review by the Director or a delegate;

6. In consultation with OGC, reviewing requests to decontrol CUI that was created or obtained by their division or office, notifying the SAO for CUI of the decision to decontrol information, and ensuring that markings and protections are removed from decontrolled CUI;

7. Working together to ensure that appropriate controls are in place to protect CUI; and

8. Ensuring that all confirmed or suspected breaches are reported immediately in accordance with this Policy and FHFA's *Information Security Incident and Personally Identifiable Information Breach Response Plan*.

H. **Contracting Officers** are responsible for ensuring that contracts and other agreements with third parties contain appropriate clauses and language requiring the protection of CUI, including any necessary clauses and prescriptions provided by the Office of Technology and Information Management.

I. **Contracting Officer's Representatives** are responsible for monitoring contractor compliance with any contract requirements regarding CUI.

J. Supervisors and Managers are responsible for:

1. Reviewing and ensuring that all CUI is properly marked in accordance with these Procedures; and

2. Ensuring that all personnel under their purview complete all required CUI training.

K. FHFA Employees and FHFA Contractor Personnel are responsible for following all policies and procedures for marking, handling, and protecting CUI; maintaining awareness at all times of CUI in their possession regardless of location (e.g., desk, office, laptops); attending annual CUI training; and ensuring that all confirmed or suspected breaches are reported immediately to FHFA's Help Desk at HelpDesk@fhfa.gov or (202) 649-3990, in accordance with this Policy.

VI. AUTHORITIES AND REFERENCES

A. *Controlled Unclassified Information*, 32 CFR Part 2002, effective 11/14/2016.

B. *Controlled Unclassified Information*, Executive Order 13556, dated 11/4/2010, (75 FR 68675).

C. NIST Special Publication 800-171, Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, dated 2/21/2020.

D. FHFA Policy No. 209 – *Information Technology Security Policy*, dated 7/23/2020 (Signed 8/7/2020).

E. FHFA Policy No. 223 – Information and Communication Technology Accessibility Policy, dated 9/11/2020.

F. FHFA Policy No. 301 – *Use and Protection of Personally Identifiable Information Policy*, dated 5/10/2022.

G. FHFA Policy No. 701 – *Facility Management Policy*, dated 9/14/2018.

H. FHFA Policy No. 1501 – *Research Dissemination Policy*, signed 2/26/2020.

I. FHFA Delegation and Designation Orders.

J. *Controlled Unclassified Information Procedures*, dated 3/20/2023**.**

K. *FHFA Information Incident and Breach Response Plan*, dated 3/29/2023.

L. FHFA *Information System Rules of Behavior and User Acknowledgment*, dated 11/2023.

VII. RECORDS RETENTION

This policy will be retained and managed in accordance with *FHFA Comprehensive Records Schedule (CRS)* Item 1.3b – Administrative Policies for 30 years. Any records created in support of administering this policy and procedures will be retained and managed in accordance with CRS Item 5.4 and destroyed or deleted when 7 years old.