Federal Housing Finance Agency
Office of Inspector General

FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines

Audit Report • AUD-2023-002 • March 8, 2023

AUD-2023-002

March 8, 2023

Executive Summary

Cloud computing is the on-demand delivery of IT resources over the internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, organizations can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider. The Federal Risk and Authorization Management Program (FedRAMP) establishes security requirements and guidelines intended to help agencies ensure that their cloud computing environments are sufficiently secure to meet the provisions of the Federal Information Security Modernization Act of 2014 (FISMA). FedRAMP leverages the National Institute of Standards and Technology's (NIST) guidelines and procedures to provide standardized security requirements for cloud services.

FHFA uses cloud services provided by contractors to process, store, or transmit certain FHFA mission-related information. FHFA established a cloud-based system (cloud system) utilizing a third-party provider's cloud computing platform to add computing resources to FHFA's on-premises computing environment. To clarify roles and responsibilities for implementing the required FedRAMP security controls, the third-party provider delineates the security responsibilities of the third-party provider and FHFA in the third-party provider's Customer Responsibility Matrix (CRM).

Within FHFA, the Office of Technology and Information Management (OTIM) works with mission and support offices to promote the effective and secure use of information and systems. We performed this audit to determine whether FHFA's oversight of its cloud system conforms with NIST requirements and FHFA standards. The audit scope focused on select security controls that FHFA is responsible for implementing as part of its oversight of its cloud system, as listed in the CRM during fiscal year (FY) 2021 (review period).

We found that FHFA did not fully implement select security controls over its cloud system as required by NIST and FHFA standards and guidelines. Specifically, we noted the following:

- FHFA did not develop a component inventory for its cloud system as required by NIST. As a result, FHFA risks not knowing which computing resources are connected to or within the boundary of its cloud system.

- A FHFA user was given privileged access to perform security-relevant functions for the cloud system without the system owner's approval,

contrary to FHFA access control requirements. Without the system owner's approval, there may be an increased risk of misuse of the cloud system.

- FHFA did not perform an annual review or update of its cloud system's System Security Plan (security plan) annually since 2018 in accordance with FHFA standards and guidelines. Consequently, FHFA's current processes and practices are not reflected in its security plan.

- FHFA did not implement encryption for all data-at-rest (e.g., data on virtual storage and databases) for its cloud system as required by NIST. Lack of encryption increases the risk of unauthorized disclosure and modification of FHFA data.

- FHFA did not perform monthly configuration compliance scans as required by FHFA standards and guidelines, increasing the likelihood that deviations from approved baseline configurations are not being detected and corrected.

When we inquired why select security controls were not fully implemented, OTIM officials stated that FHFA lacked the resources necessary to implement the required security controls during the review period. OTIM officials subsequently informed us that they hired an IT specialist in April 2022 to assist with developing the component inventory, updating the security plan, and conducting monthly compliance scans for its cloud system. OTIM officials stated that, since being hired, the IT specialist has developed a component inventory, initiated updating the cloud system's security plan, created a plan to encrypt all data-at-rest, and conducted monthly configuration compliance scans. We found that OTIM has either initiated or planned for the implementation of these security controls but has not yet fully implemented them.

We made six recommendations in this report. In a written response, FHFA management agreed with our recommendations.

This report was prepared by Jackie Dang, IT Audit Director; Marcie McIsaac, IT Audit Manager; and Zachary Lewkowicz, Auditor-in-Charge; with assistance from Abdil Salah, Assistant Inspector General for Audits. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report.

AUD-2023-002

March 8, 2023

This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov and www.oversight.gov.

James Hodge, Deputy Inspector General for Audits /s/

TABLE OF CONTENTS

ABBREVIATIONS

CIS	Center for Internet Security
CRM	Customer Responsibility Matrix
Enterprises	Fannie Mae and Freddie Mac
FedRAMP	Federal Risk and Authorization Management Program
FHFA or Agency	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
NIST	National Institute of Standards and Technology
OTIM	Office of Technology and Information Management
POA&M	Plans of Action and Milestones
Regulated Entities	Fannie Mae, Freddie Mac, any affiliate of Fannie Mae and Freddie Mac, and the Federal Home Loan Banks
SP	Special Publication

BACKGROUND

FHFA's Network and Cloud Systems

FHFA's network and systems host a variety of data and information such as financial reports, data from the Enterprises, examinations and analyses of the regulated entities, and personally identifiable information of employees. FHFA's general support system provides connectivity between the Agency's sites, headquarters, and data centers, as well as internet access, email, and directory services for all Agency divisions and offices.

FHFA uses cloud services provided by contractors to process, store, or transmit certain FHFA mission-related information. FHFA established a cloud system utilizing a third-party provider's cloud computing platform to add computing resources to FHFA's on-premises computing environment. During FY 2021, FHFA owned a total of 41 systems, 20 of which were cloud systems.

Third-Party Provider and FHFA Cloud Security Responsibilities

The third-party provider and FHFA share the responsibility for security for the cloud-based systems, as delineated in the third-party provider's CRM. The third-party provider is responsible for protecting the infrastructure that runs all of the services offered in the third-party provider's cloud. This infrastructure is composed of the hardware, software, network, and facilities that run the third-party provider's cloud services. FHFA is responsible for, among other things, the following five security controls as outlined in the NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Information Systems and Organizations*, updated January 2015 (NIST SP 800-53):[1]

- Component inventory – NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, updated October 2019, defines a component inventory as a descriptive record of components within an information system. NIST SP 800-53 defines an information system component as "[a] discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system." To assemble and maintain an accurate inventory of information system components, agencies must define the basic information to be collected, such as hardware specifications (manufacturer, device type, model, serial number, physical location), software license information, software

[1] NIST SP 800-53, Revision 4, is applicable for our review period.

version numbers, and component owners, then review and update the component inventory on a regular basis.

- Access control – NIST SP 800-53 defines access control as the process of granting or denying specific requests for obtaining and using information and related information processing services, and for entering specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances).

- Risk assessment – NIST SP 800-53 defines risk assessment as the process of identifying risks to organizational operations (including mission, functions, image, and reputation), assets, individuals, other organizations, and the nation, resulting from the operation of an information system. Risk assessment is a component of risk management and incorporates threat and vulnerability analyses. Security plans document risk assessment of security controls that are in place. NIST SP 800-53 further explains that security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements.

- Data protection – NIST SP 800-53 defines data-at-rest[2] as the state of information when it is located on storage devices as specific components of information systems. NIST SP 800-53 defines protection of data-at-rest as a control that addresses the confidentiality and integrity of information at rest and covers user information and system information. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning.

- Configuration management – NIST SP 800-53 defines configuration management as activities that focus on establishing and maintaining the integrity of information systems through control of processes for initializing, changing, and monitoring the configurations of systems.

[2] Data-at-rest refers to the state of information when it is not in process or in transit and is located on system components.

Federal Standards Applicable to FHFA's Cloud System

FedRAMP[3] establishes security requirements and guidelines intended to help agencies ensure that their cloud computing environments are sufficiently secured to meet the provisions of FISMA. Among other things, FISMA requires federal agencies, including FHFA, to develop, document, and implement an information security program, and evaluate the program's effectiveness. FISMA also requires agencies to ensure the security of information and systems maintained by or on behalf of the agency. The law also applies to systems used or operated by a contractor or other organization on behalf of the agency, such as information technology resources provided via cloud services. In addition, FISMA requires federal agencies to comply with mandatory information security standards and guidelines, as well as mandatory standards developed by NIST.

The relevant NIST SP 800-53 technical specifications require that federal agencies perform the following:

- Develop and document a component inventory that accurately reflects the current system, includes all components within the authorization boundary of the information system, and is at the granularity deemed necessary for tracking and reporting.
- Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
- Implement cryptographic mechanisms[4] to prevent unauthorized disclosure and modification of the data-at-rest.

FHFA's Standards and Guidelines Applicable to Its Cloud Systems

FHFA has several written policies and procedures that govern its processes related to information security that include, among other things, configuration management standards, vulnerability management process, and a system security plan. Specifically:

[3] FedRAMP's mission is to promote the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessment. Managed by the General Services Administration, the program aims to ensure that cloud computing services have adequate information security, while also eliminating duplicative efforts and reducing operational costs.

[4] Cryptographic mechanisms provide confidentiality, integrity, source authentication, and access control (e.g., encryption and decryption, and digital signature generation and verification).

- FHFA's secure configuration management standard requires monthly configuration compliance scans to check assets and software of its cloud system for compliance with configuration benchmarks.

- FHFA's cloud system's security plan states the system owner[5] is responsible for approving requests to create information system accounts, including requests for access of privileged users.[6] Additionally, the security plan requires an annual review and being updated whenever there are significant changes to the system. Furthermore, the security plan requires that all data-at-rest is encrypted.

FACTS AND ANALYSIS

In Oversight of Its Cloud System, FHFA Did Not Fully Implement Select Security Controls in Accordance with NIST Standards and Its Own Standards and Guidelines

We found that FHFA did not fully implement select security controls over its cloud system as required by NIST and FHFA standards and guidelines. Specifically, we noted that (1) FHFA did not develop the component inventory for its cloud system; (2) a FHFA user was also given privileged access to perform security-relevant functions for the cloud system without the system owner's approval; (3) FHFA did not perform an annual review or update to its cloud system's security plan for more than three years (i.e., since 2018);[7] (4) FHFA did not implement encryption for all data-at-rest (e.g., data stored on virtual storage and databases) for its cloud system; and (5) FHFA did not perform monthly configuration compliance scans. OTIM officials stated that these issues occurred because they lacked the resources required to implement the required security controls. These issues raise concerns about the effectiveness of FHFA's oversight of its cloud system. To illustrate:

1. Component Inventory. FHFA did not develop component inventory for its cloud system as required by NIST SP 800-53. Instead, FHFA used the cloud system's monthly billing statements as its system component inventory. OTIM officials acknowledged that the current billing statements were not an accurate inventory. Without a fully developed component inventory, FHFA runs the risk of not knowing

[5] A system owner is an Agency official responsible for defining the operating parameters, authorized functions, and security requirements of an information system.

[6] A privileged user is someone authorized, and therefore trusted, to perform security-relevant functions that ordinary users are not authorized to perform.

[7] FHFA last reviewed and updated its cloud's security plan on August 10, 2018. As of September 30, 2021 (end of our review period), FHFA did not review the security plan at least annually or update the plan for significant changes to the cloud system.

which computing resources are connected to or within the boundary of its cloud system. When interviewed, OTIM officials stated that they did not have resources to create, update, and maintain a component inventory. Subsequently, OTIM officials informed us that an IT specialist was hired in April 2022 who has developed a component inventory. Based on our review of the new component inventory OTIM provided, we determined that the inventory was not yet fully developed and missing components of the cloud system.

2. Access Control. FHFA continuously monitored access to its cloud system as required by its own standard. However, a FHFA user was given privileged access to perform security-relevant functions for the cloud system without the system owner's approval. Giving users privileged access to perform security-relevant functions for the cloud system without proper approval may increase the risk of potential misuse of the cloud system. OTIM officials stated that FHFA allowed security group owners[8] to approve access requests to the third-party provider's cloud management console;[9] therefore, the system owner did not have to approve this access request. According to OTIM officials, the cloud system's security plan may need to be updated to reflect this process.

3. Risk Assessment. FHFA did not perform an annual review or update to its cloud system's security plan since 2018, contrary to its own requirement. For example, the security plan did not include statements describing FHFA's implementation of cryptographic protection. In addition, the security plan did not reflect the current security processes for offboarding cloud system users, such as removing access. Without an updated security plan, FHFA may not be able to provide an accurate overview of the security requirements of its cloud system or describe the current controls in place. In a written statement, OTIM officials stated that this occurred due to a lack of resources. OTIM officials stated that the IT specialist hired in April 2022 has initiated updating the cloud system's security plan. Although our audit found that

[8] A security group is a collection of user accounts that are assigned with the same access rights to shared computing resources (e.g., shared folders, files, servers, and printers). Security group owners add or remove users from a security group.

[9] The third-party provider's cloud management console is a web application that comprises and refers to a broad collection of service consoles for managing the third-party provider's cloud resources.

OTIM had not completed updating the security plan, it has developed plans of action and milestones (POA&M)[10] to do so.

4. Data Protection. FHFA encrypted data in-transit for its cloud system but did not implement encryption for all data-at-rest as required by NIST SP 800-53. Specifically, we found and verified with OTIM staff that 25% of storage buckets[11] and 66% of relational databases[12] were not implementing encryption for data-at-rest. OTIM officials stated that some of the storage buckets were being encrypted as part of the data backup process;[13] therefore, OTIM did not need to encrypt these storage buckets. OTIM officials also stated that no options were provided by the third-party provider to encrypt data-at-rest in some of their relational databases. We found and confirmed with the third-party provider that options are available for encrypting data-at-rest in these relational databases and the customer is responsible for encrypting all data-at-rest. We informed OTIM officials about these available encryption options and customer responsibilities. Without encryption of data-at-rest, FHFA's information residing on its cloud system could be at risk of unauthorized disclosure and modification. In a written statement, OTIM officials subsequently stated they did not have the resources to plan, test, and deploy an enterprise-wide key management solution to address the overall encryption issue. OTIM officials later informed us that the IT specialist hired in April 2022 has created a plan to encrypt all data-at-rest. During the course of the audit, we determined that OTIM did not implement encryption for all data-at-rest.

5. Configuration Management. FHFA did not perform monthly configuration compliance scans as required by its own standards. During our audit, we requested FY 2021 cloud system configuration compliance scans. Instead, FHFA provided two

[10] POA&M are management tools that describe the planned actions to correct information system security and privacy weaknesses in controls identified during audits, assessments of controls, or continuous monitoring activities. POA&M include: tasks to be accomplished; resources required to accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the milestones and tasks. The key purpose of POA&M is to facilitate a disciplined and structured approach to account for and mitigate all known risks related to security weaknesses in accordance with an organization's priorities.

[11] To store data in the third-party provider's simple storage service, customers work with resources known as buckets and objects. A bucket is a container for objects. An object is a file and any metadata that describes that file. For example, to store an object in the third-party provider's simple storage service, customers create a bucket and then upload the object to a bucket. When the object is in the bucket, the customer can open it, download it, and move it.

[12] The third-party provider's relational database service is a web service that allows customers to set up and operate relational databases in the cloud. For example, relational databases can be thought of as a collection of spreadsheet files that help businesses organize, manage, and relate data. In the relational database model, each "spreadsheet" is a table that stores information, represented as columns (attributes) and rows (records).

[13] A backup is a copy of files and programs to facilitate recovery if necessary.

reports from configuration compliance scans conducted in March 2020 and April 2022. OTIM officials acknowledged that FHFA did not perform cloud system configuration compliance scans during FY 2021. By not conducting FHFA required monthly configuration compliance scans, there is an increased likelihood that deviations from approved baseline configurations may not be detected and corrected. According to OTIM officials, they did not have the resources to perform the cloud system configuration compliance scans during the audit period. In a technical comment to this report, OTIM asserted the IT specialist hired in April 2022 has since conducted monthly configuration compliance scans. We did not validate OTIM's assertion because OTIM did not provide us with the monthly configuration compliance scan reports. In a meeting that was held after we provided management a copy of a draft of this report for technical comments, OTIM officials informed us that they have initiated conducting configuration compliance scans in September 2022 and agreed to provide us evidence of their corrective actions after the issuance of the final report.

FINDINGS

- FHFA did not develop its cloud system component inventory as required by NIST SP 800-53.
- A FHFA user was given privileged access to perform security-relevant functions for the cloud system without the system owner's approval, contrary to FHFA's access control requirements.
- FHFA did not update its cloud system's security plan annually since 2018 as required by FHFA standards and guidelines.
- FHFA did not implement encryption for all data-at-rest for its cloud system as required by NIST SP 800-53.
- FHFA did not perform monthly configuration compliance scans as required by FHFA standards and guidelines.

CONCLUSIONS

We identified multiple exceptions to federal requirements and FHFA standards and guidelines regarding FHFA's oversight of its cloud system and implementation of select security

controls for which FHFA management is responsible. In our view, these exceptions occurred with sufficient frequency to warrant heightened management attention to the cybersecurity risk posed to its cloud system.

RECOMMENDATIONS

We recommend that the Acting Chief Information Officer at FHFA:

1. Assess whether OTIM has sufficient qualified staff to complete required oversight of FHFA's cloud system to meet NIST and FHFA requirements, and address any resource constraints that have adversely affected OTIM's ability to implement security controls for its cloud system, including component inventory, access control, risk assessment, data protection, and configuration management requirements.

2. Develop and maintain a complete and accurate cloud system component inventory, as required by NIST SP 800-53.

3. Ensure that privileged user access is appropriately approved in accordance with FHFA standards and guidelines.

4. Update the cloud system's security plan to include FHFA's current processes and implementation of all current NIST security controls, and ensure the security plan is reviewed annually.

5. Develop and implement a solution to encrypt all data-at-rest on the cloud system as required by NIST SP 800-53.

6. Ensure that cloud system configuration compliance scans are conducted monthly as required by FHFA standards and guidelines.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA management an opportunity to respond to a draft of this audit report. FHFA management provided technical comments that were considered in finalizing this report. FHFA management also provided a written management response, which is included as an Appendix to this report. In its response, FHFA management agreed with our recommendations. The following summarizes FHFA's responses and our comments.

FHFA Comments to Recommendation 1

FHFA agreed with this recommendation. Management responded that OTIM hired a Cloud Security Engineer in April 2022 to address the initial resource constraint specific to FHFA's cloud initiatives and relevant security requirements. Further, management stated that as OTIM continues to evaluate its overall staffing needs and resource constraints, OTIM will request additional resources if the assessment finds that resource constraints continue to impact OTIM's ability to meet NIST and FHFA requirements. OTIM will complete this assessment by June 30, 2023.

OIG Response to FHFA Comments to Recommendation 1. Management's response meets the intent of our recommendation.

FHFA Comments to Recommendation 2

FHFA agreed with this recommendation. Management responded that, as of June 2022, OTIM automated the delivery of a complete and accurate monthly cloud system component inventory and will provide evidence to OIG no later than March 31, 2023.

OIG Response to FHFA Comments to Recommendation 2. Management's response meets the intent of our recommendation.

FHFA Comments to Recommendation 3

FHFA agreed with this recommendation. Management responded that OTIM will review and, if necessary, revise the privileged user access approval process documented in its Cloud System Security and Privacy Plan to ensure that this process follows FHFA's standards and guidelines, and communicate the revised process to all stakeholders. This will be completed by December 31, 2023.

OIG Response to FHFA Comments to Recommendation 3. Management's response meets the intent of our recommendation.

FHFA Comments to Recommendation 4

FHFA agreed with this recommendation. Management responded that OTIM will update the cloud system security and privacy plan by December 31, 2023.

OIG Response to FHFA Comments to Recommendation 4. Management's response meets the intent of our recommendation.

FHFA Comments to Recommendation 5

FHFA agreed with this recommendation. Management responded that OTIM developed a Cloud Key Management Plan, pending approval of the Testing and Change Control Board. OTIM will encrypt applicable cloud services. This will be completed by January 31, 2024.

OIG Response to FHFA Comments to Recommendation 5. Management's response meets the intent of our recommendation.

FHFA Comments to Recommendation 6

FHFA agreed with this recommendation. Management responded that, as of September 2022, OTIM conducted monthly configuration compliance scans for its cloud system using industry-accepted benchmarks and will provide evidence to OIG no later than March 31, 2023.

OIG Response to FHFA Comments to Recommendation 6. Management's response meets the intent of our recommendation.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

Our objective for this audit was to determine whether FHFA's oversight of the cloud system conforms with NIST requirements and FHFA standards. As part of this audit, we tested select security controls that FHFA is responsible for implementing for its cloud system as listed in the Customer Responsibility Matrix (CRM) as part of its oversight during FY 2021. We selected the following five security controls outlined in the NIST requirements and the 18 CIS [Center for Internet Security] Critical Security Controls:[14] component inventory, access control, risk assessment, data protection, and configuration management. Our review period was from October 1, 2020, through September 30, 2021.

To accomplish our objective, we:

- Determined that two components of Government Accountability Office (GAO)'s *Standards for Internal Control in the Federal Government* were significant to our objective: (1) control activities, and the underlying principles that management should design the entity's information system and related control activities to achieve objectives and respond to risks, and design control activities for appropriate access to protect the entity's information system; and (2) enforce accountability, and the

[14] CIS is a nonprofit organization dedicated to enhancing cyber security readiness of public and private sector entities. The 18 CIS Security Controls are high-priority and highly effective defensive actions that provide a "must-do, do-first" starting point for every enterprise seeking to improve its cyber defense.

underlying principle that management holds service organizations accountable for their assigned internal control responsibilities.

- Reviewed the following NIST publications:
  - Reviewed NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, updated January 2015
  - NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- Reviewed the following FHFA policies and procedures:
  - FHFA secure configuration management standards
  - FHFA FY 2021 and FY 2022 vulnerability management process
  - FHFA's cloud system's security plan
- Reviewed the third-party provider's CRM for security controls that FHFA is responsible for implementing for its cloud system.
- Reviewed the system and organization controls 2 (SOC 2) type 2 report that examines the security, availability, and confidentiality of the service provider's cloud computing platform for the period of April 1, 2021, through September 30, 2021.
- Reviewed the 18 CIS Critical Security Controls.
- Obtained, reviewed, and analyzed FHFA's cloud system documentation and determined whether FHFA followed NIST SP 800-53 and FHFA standards for issuing the authority to operate and implementing continuous monitoring for the cloud system.
- Obtained, reviewed, and analyzed FHFA's cloud system documentation and determined whether FHFA implemented action in the following areas (designated in the CRM as a customer control) as required by NIST SP 800-53:
  - Component inventory
  - Access controls
  - Risk assessment
  - Data protection controls

- Configuration management controls as required by NIST SP 800-53, FHFA's cloud system's security plan, and FHFA's secure configuration standards

- Interviewed OTIM officials and staff regarding FHFA's oversight of the cloud system.

- We conducted this performance audit between October 2021 and March 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX: FHFA MANAGEMENT RESPONSE.....

This page intentionally blank. See the following page(s).

Federal Housing Finance Agency

MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audit

THROUGH: Katrina D. Jones, Chief Operating Officer

FROM: Tammy L. Tippie, Acting Chief Information Officer

KATRINA JONES — Digitally signed by KATRINA JONES Date: 2023.02.21 09:40:50 -05'00'

TAMMY TIPPIE — Digitally signed by TAMMY TIPPIE Date: 2023.02.21 09:41:55 -05'00'

SUBJECT: Draft Audit Report: *FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines*

DATE: February 21, 2023

Thank you for the opportunity to respond to the above-referenced draft audit report by the Office of Inspector General (OIG). This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the six recommendations in the draft report.

Recommendation 1: *Assess whether OTIM has sufficient qualified staff to complete required oversight of FHFA's cloud system to meet NIST and FHFA requirements, and address any resource constraints that have adversely affected OTIM's ability to implement security controls for its cloud system, including component inventory, access control, risk assessment, data protection, and configuration management requirements.*

Management Response: FHFA agrees with Recommendation 1. OTIM's Information Technology Security Branch identified a resource constraint specific to FHFA's cloud initiatives and relevant security requirements and requested a Cloud Security Engineer position. The Cloud Security Engineer position was approved and staffed in April 2022. This FTE has addressed the initial resource constraint identified by OTIM. OTIM continues to evaluate its overall staffing needs and the adverse effects of resource constraints. OTIM will request additional resources if the assessment finds that resource constraints continues to impact OTIM's ability to meet NIST and FHFA requirements. FHFA will complete this assessment by June 30, 2023.

Recommendation 2: *Develop and maintain a complete and accurate cloud system component inventory, as required by NIST SP 800-53.*

Management Response: FHFA agrees with Recommendation 2. As of June 2022, FHFA has automated the delivery of a complete and accurate monthly cloud system component inventory. FHFA will provide evidence to the OIG no later than March 31, 2023.

Recommendation 3: *Ensure that privileged user access is appropriately approved in accordance with FHFA standards and guidelines.*

Management Response: FHFA agrees with Recommendation 3. FHFA will review the privileged user access approval process documented in its Cloud System Security and Privacy Plan, and if necessary, revise this component of the plan (as part of FHFA's overall update to the plan) to ensure that the privileged user access approval process follows FHFA's standards and guidelines, and communicated to all stakeholders. This will be completed by December 31, 2023.

Recommendation 4: *Update the cloud system's security plan to include FHFA's current processes and implementation of all current NIST security controls and ensure the security plan is reviewed annually.*

Management Response: FHFA agrees with Recommendation 4. FHFA will update the cloud system security and privacy plan by December 31, 2023.

Recommendation 5: *Develop and implement a solution to encrypt all data-at-rest on the cloud system as required by NIST SP 800-53.*

Management Response: FHFA agrees with Recommendation 5. FHFA has developed a Cloud Key Management Plan and will begin to encrypt applicable cloud services following the successful Testing and Change Control Board approval as required by FHFA's Change Management Procedures. This will be completed by January 31, 2024.

Recommendation 6: *Ensure that cloud system configuration compliance scans are conducted monthly as required by FHFA standards and guidelines.*

Management Response: FHFA agrees with Recommendation 6. As of September 2022, FHFA implemented a monthly cloud system configuration compliance scan using industry accepted benchmarks. FHFA will provide evidence to the OIG no later than March 31, 2023.

If you have questions, please contact Stuart Levy at (202) 649-3610 or e-mail, Stuart.Levy@fhfa.gov.

CC:

John Major
Ralph Mosios
Jim Vercellone

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

  FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219