Federal Housing Finance Agency
Office of Inspector General

FHFA Failed to Follow its Cloud-Based Computing Requirements when it Did Not Validate the Implementation of Minimum Security Requirements for Cloud-Based Tools and Did Not Include Required IT Security Provisions in Some of its Cloud Service Contracts

Audit Report • AUD-2020-013 • September 17, 2020

AUD-2020-013

September 17, 2020

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency), established by the Housing and Economic Recovery Act of 2008, is responsible for the supervision, regulation, and housing mission oversight of Fannie Mae and Freddie Mac (together, the Enterprises), and the Federal Home Loan Bank System (FHLBanks) (collectively, the regulated entities), and the FHLBanks' fiscal agent, the Office of Finance. Since 2008, FHFA has served as conservator of the Enterprises.

FHFA uses cloud services provided by contractors to process, store, or transmit certain FHFA mission-related and non-mission related information. FHFA also uses a number of cloud security tools provided by contractors to assist in the oversight and management of its General Support System (GSS). FHFA's acquisition procedures directs that an information technology (IT) security clause is included in contracts for externally hosted information systems operated by a contractor on behalf of FHFA. In April 2018, FHFA established a methodology to prioritize resources on information systems, including those in the cloud, that present the greatest risk to the Agency. Among other things, for cloud-based GSS tools, the methodology requires the validation of the implementation of minimum security requirements and the inclusion of IT security provisions in cloud service contracts.

We conducted this audit to determine whether FHFA followed its policies for cloud-based IT services. Our review period was April 2018 through April 2020.

We found that FHFA failed to follow its methodology by not validating the implementation of the minimum security requirements for its cloud-based GSS tools. We also found that FHFA did not include the required IT security provisions in some cloud service contracts.

Based on our findings in this audit, we make three recommendations in this report. In a written management response, FHFA agreed with our recommendations.

This report was prepared by Jackie Dang, Audit Director; Dan Jensen, Auditor-in-Charge; with assistance from Abdil Salah, Assistant Inspector General for Audits; and Bob Taylor, Senior Advisor. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report.

AUD-2020-013

September 17, 2020

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.

Marla A. Freedman, Senior Audit Executive /s/

TABLE OF CONTENTS ....

ABBREVIATIONS

ATO	Authorization to Operate
CIO	Chief Information Officer
FedRAMP	Federal Risk and Authorization Management Program
FHFA or Agency	Federal Housing Finance Agency
FHLBank	Federal Home Loan Bank
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
GSS	General Support System
IS Characterization Methodology	Information System Characterization Methodology memorandum
IT	Information Technology
NIST	National Institute of Standards and Technology
OBFM	Office of Budget and Financial Management
OIG	Federal Housing Finance Agency Office of Inspector General
OMB	Office of Management and Budget
OTIM	Office of Technology and Information Management
SP	Special Publication

BACKGROUND..

FHFA's Network and Systems

FHFA's network and systems process and host 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 GSS is a wide area network that provides connectivity, information sharing and data processing capabilities, remote and network access, and security and support services.

FHFA's Office of Technology and Information Management (OTIM) works with mission and support offices to promote the effective and secure use of information and systems.

Federal Cloud Computing Strategies and Resources

To accelerate the Federal Government's use of cloud computing, in 2011 the White House adopted a "Cloud First" policy.[1] The Federal Cloud Computing Strategy (the Cloud First Policy)[2] was released in 2011 to help agencies identify services suitable for moving to the cloud and provide a framework for making the transition. It also required agencies to consider cloud solutions first for any new acquisitions.

To help Federal agencies meet the Cloud First Policy, the General Services Administration, National Institute of Standards and Technology (NIST), the Departments of Defense and Homeland Security, and other stakeholders collaborated to establish the Federal Risk and Authorization Management Program (FedRAMP). 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.

FedRAMP establishes security requirements and guidelines that are intended to help secure cloud computing environments used by agencies and to meet the provisions of the Federal Information Security Modernization Act of 2014 (FISMA) and implementing guidance. FedRAMP's security requirements and guidelines specify the actions agencies and cloud service providers should take to authorize cloud services through the program. Further, the Office of Management and Budget (OMB) requires agencies to authorize information systems

[1] The Cloud First Policy was intended to accelerate the pace at which the Federal Government realized the value of cloud computing by requiring agencies to evaluate safe, secure, cloud computing options before making any new investments.

[2] U.S. Chief Information Officer, *Federal Cloud Computing Strategy* (Feb. 2011).

prior to their operation and periodically thereafter. This requirement also applies to the use of cloud services.[3] OMB required that by June 2014, executive branch agencies use FedRAMP for authorizing cloud services. Additionally, OMB required, among other things, that each executive department or agency:

- Use FedRAMP when conducting risk assessments, security authorizations, and granting authorization to operate (ATO)[4] for all executive department or agency use of cloud services;
- Ensure applicable contracts appropriately require cloud service providers to comply with FedRAMP security authorization (i.e., ATO) requirements; and
- Ensure that acquisition requirements address maintaining FedRAMP security authorization requirements and that relevant contract provisions related to contractor reviews and inspections are included for cloud service providers.[5]

In 2019, OMB published a new strategy to accelerate agency adoption of cloud-based solutions: Cloud Smart.[6] The Cloud Smart strategy instructs that Federal agencies should assess the need for and usage of applications and discard obsolete, redundant, or overly resource-intensive applications. Agencies should assess their requirements and seek the environments and solutions, cloud or otherwise, that achieve their mission goals while being good stewards of taxpayer resources. Additionally, agencies need to place security and privacy considerations at the forefront of procurement efforts.

- Any federal agencies considering adoption of cloud computing systems must adhere to the standards adopted by NIST. Among other things, NIST requires federal agencies to implement controls on information systems according to their impact, including formally authorizing those systems to operate.[7]

[3] OMB, Circular A-130, *Managing Information as a Strategic Resource* (July 2016). The circular states: "FISMA requires each agency to provide information security for the information and 'information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.' This includes services that are either fully or partially provided, including agency-hosted, outsourced, and **cloud-based solutions**." (emphasis added)

[4] An ATO is the official management decision given by a senior official to authorize operation of an information system and explicitly accept the risk to operations, assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

[5] Federal Chief Information Officer memorandum dated December 8, 2011, "Security Authorization of Information Systems in Cloud Computing Environments."

[6] U.S. Federal Chief Information Officer, *Federal Cloud Computing Strategy* (June 2019).

[7] NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013, updated Jan. 2015).

FHFA's Acquisition Procedures Manual – Applicable Requirements for Cloud Computing Services Contracts

FHFA's Acquisition Procedures Manual, dated June 26, 2019, directs FHFA's contracting officers to use certain contract clauses as applicable, including an IT security clause for acquisitions of externally hosted information systems operated by a contractor on behalf of FHFA. Any externally hosted cloud computing systems used by FHFA would be subject to this IT security clause. The IT security clause, among other things, includes provisions that: (1) IT products and services provided by the contractor comply with federal laws and standards, including but not limited to NIST requirements; and (2) the right of FHFA, the FHFA Office of Inspector General (OIG), and the Government Accountability Office (GAO) to evaluate the contractor's security controls or privacy practices.[8]

According to OTIM and the Office of Budget and Financial Management (OBFM) officials, FHFA's contracting process starts with the acquiring office identifying its requirements before meeting with OBFM to finalize all contract requirements. The Acquisition Procedures Manual and supplementary instructions identify required solicitation and contract clauses, in addition to the requirements from OTIM and OBFM, to be included for certain acquisitions, such as cloud computing systems. The contracting documents are to be reviewed by OTIM to ensure the requisite IT security requirements are present.

OTIM's Methodology for Characterizing Information Systems as "FISMA Reportable," "GSS Tool," and "Non-FISMA Reportable"

- In March 2018, OTIM Security prepared a staff analysis memorandum, "Information System Characterization Methodology" (IS Characterization Methodology), that established a methodology for FHFA to prioritize resources on protecting information and systems that present the greatest risk to the Agency, including information systems in the cloud. In April 2018, FHFA's Chief Information Officer (CIO), Chief Information Security Officer, Chief Technology Officer, and Senior Agency Official for Privacy approved the IS Characterization Methodology. As the IS Characterization Methodology explains, "FHFA is applying adequate security and protecting information systems commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." That methodology established the following designations for information systems:

[8] FHFA, *Acquisitions Procedures Manual*, Version 2019.01 (June 26, 2019), Special Clauses and Provisions 6.208d "IT Security clause for acquisitions of information systems operated by a Contractor on behalf of FHFA." Similar provisions regarding contractor compliance with Federal IT security requirements and rights of FHFA, OIG, and GAO to evaluate contractor security controls and privacy practices were in prior versions of the manual in effect during our review period.

- FISMA Reportable Information System: This designation will be attached to information systems used to process, store, or transmit FHFA mission-related information, or non-mission related information categorized at the moderate or high impact level. For information systems designated as FISMA Reportable Information Systems, the IS Characterization Methodology requires a Security Assessment and Authorization and an ATO be completed before the system is placed into operation.

- GSS Tool: This designation will be attached to a system or service that assists in the oversight and management of the GSS and supports FHFA's implementation of one or more NIST SP 800-53 security controls. GSS Tools do not store FHFA mission-related data. For cloud-based GSS Tools, the IS Characterization Methodology requires the inclusion of minimum security requirements as part of the contract Statement of Work and requires OTIM to validate the implementation of minimum security requirements. An ATO is not required for GSS Tools.

- Non-FISMA Reportable System: This designation will be attached to a system or service used by FHFA's administrative/support offices for non-mission related purposes, such as the automation of an administrative manual process that stores, processes, or transmits low impact data. Non-FISMA Reportable Systems are not within the scope of this audit.

FHFA's Cloud Services Inventory as of April 2020 and its Cloud Strategy Going Forward

FHFA reported to us that as of April 2020, its cloud services inventory consisted of 10 FISMA Reportable Information Systems and 8 GSS Tools.

In April 2020, FHFA's CIO approved the FHFA Cloud Computing Strategy, which was consistent with Cloud Smart. The FHFA strategy provides guidance for future migrations to cloud services and lays out conditions under which transferring existing services to the cloud would be considered (e.g., IT staff departures, aging hardware, versions of applications no longer supported, major upgrades), as well as when to use the cloud for future services.[9] According to the strategy, "[OTIM] has created this document to explain what 'The Cloud' is, why it has become so integral to IT service delivery, and how we are adopting, integrating, and migrating to 'The Cloud' at FHFA."

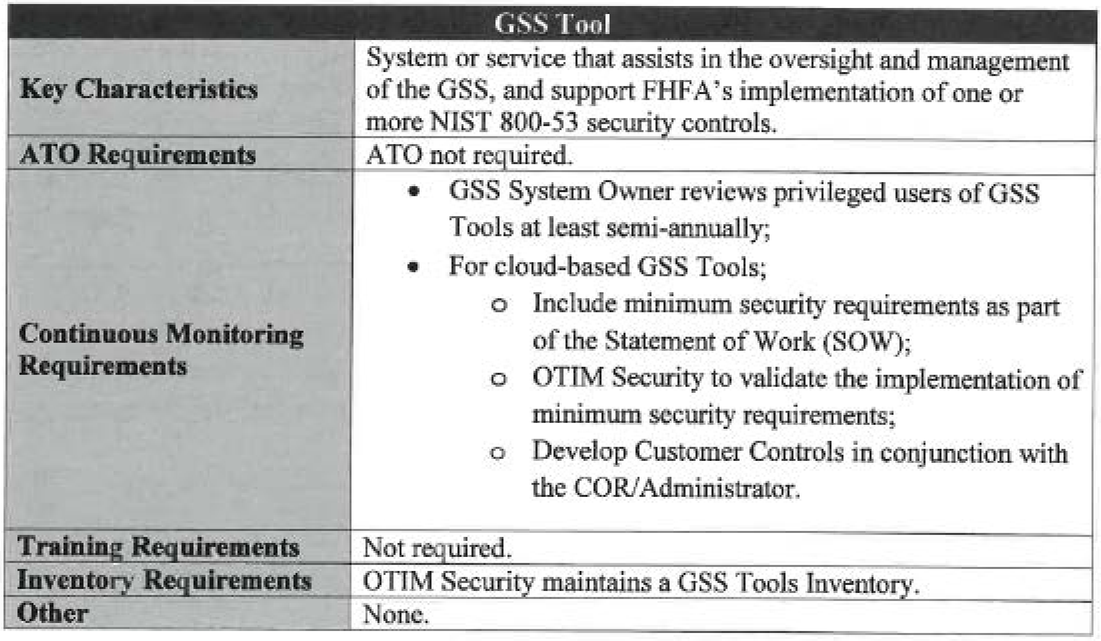
[9] The 18 cloud services that are the subject of this audit were already in place before the April 2020 cloud strategy was approved.

FACTS AND ANALYSIS ....

FHFA Failed to Follow its Methodology when it Did Not Validate the Implementation of Minimum Security Requirements for Cloud-Based GSS Tools and Did Not Include Required IT Security Provisions in Some of its Cloud Service Contracts

FHFA's CIO, Chief Information Security Officer, Chief Technology Officer, and Senior Agency Official for Privacy approved the IS Characterization Methodology. As explained, this methodology does not require an ATO for GSS Tools. See Figure 1 below.

FIGURE 1. GSS TOOL CHARACTERISTICS



	GSS Tool
Key Characteristics	System or service that assists in the oversight and management of the GSS, and support FHFA's implementation of one or more NIST 800-53 security controls.
ATO Requirements	ATO not required.
Continuous Monitoring Requirements	• GSS System Owner reviews privileged users of GSS Tools at least semi-annually; • For cloud-based GSS Tools; ○ Include minimum security requirements as part of the Statement of Work (SOW); ○ OTIM Security to validate the implementation of minimum security requirements; ○ Develop Customer Controls in conjunction with the COR/Administrator.
Training Requirements	Not required.
Inventory Requirements	OTIM Security maintains a GSS Tools Inventory.
Other	None.

Source: IS Characterization Methodology

OTIM Did Not Validate the Implementation of Minimum Security Requirements for Cloud-Based GSS Tools, Contrary to the Requirements of the IS Characterization Methodology

The IS Characterization Methodology directs that OTIM Security shall validate the implementation of minimum security requirements for cloud-based GSS Tools. See Figure 1 above. OTIM provided no documentary evidence that it validated the minimum security requirements for any of FHFA's cloud-based GSS Tools. OTIM officials asserted that they decided not to perform security assessments for cloud-based GSS Tools because they said it was an inefficient use of Agency resources, notwithstanding the contrary direction in the methodology.

FHFA Did Not Include Required IT Security Provisions in Some of Its Cloud Service Contracts

FHFA's Acquisition Procedures Manual requires that the contract terms for acquisitions of information systems operated by a contractor on behalf of FHFA include, among other applicable requirements, two provisions: (1) the contractor comply with federal laws and standards addressing information security, including requirements set forth by NIST, and (2) the right of FHFA, OIG, and GAO to evaluate the security controls and privacy practices implemented by the contractor under the contract.

For the cloud-based FISMA Reportable Information Systems, the contract for one of the ten systems lacked the required provision for FHFA, OIG, and GAO rights to evaluate the contractor's security controls and privacy practices. While an OTIM Security staff person attributed the missing provision to an oversight, the Acquisition Procedures Manual directs that contracting documents should be reviewed by OTIM to ensure the requisite IT security requirements are present.

We recognize that FHFA accepted certain risk by not requiring an ATO for its cloud-based GSS Tools and imposed two compensating controls in contracts for cloud-based GSS Tools to mitigate that risk: contract provisions for minimum security requirements and the right for OTIM (and OIG and GAO) to validate the cloud service provider's implementation of minimum security requirements. We found that six of the eight contracts for cloud-based GSS Tools reviewed in this audit lacked both compensating controls.

OTIM officials contended that the lack of a required ATO for GSS Tools meant that these compensating controls were not mandatory. That claim demonstrates a misunderstanding of the required compensating controls for contracts for cloud-based GSS Tools. The IS Characterization Methodology instructs: "For cloud-based GSS Tools [i]nclude minimum security requirements as part of the Statement of Work…". See Figure 1 above. FHFA's Acquisition Procedures Manual directs the contracting officer to include these provisions in any contract related to IT security where FHFA is acquiring externally hosted cloud services operated by a contractor.

FINDINGS ....

- OTIM did not validate the implementation of the minimum security requirements for cloud-based GSS Tools, contrary to the requirements of the IS Characterization Methodology.

- FHFA did not include required IT security provisions in some of its cloud service contracts.

CONCLUSION...

FHFA failed to follow its IS Characterization Methodology by not validating the implementation of the minimum security requirements for its cloud-based GSS Tools, nor including the required IT security provisions in some cloud service contracts.

RECOMMENDATIONS...

We recommend that FHFA:

1. Validate the implementation of minimum security requirements for all existing cloud-based GSS Tools and ensure to do the same for future cloud-based GSS Tools.

2. Modify existing cloud-based GSS Tool contracts to include the required IT security provisions and ensure future cloud-based GSS Tool contracts include all required provisions.

3. Reinforce the requirements in the IS Characterization Methodology to OTIM Security staff.

FHFA COMMENTS AND OIG RESPONSE.....................................

We provided FHFA an opportunity to respond to a draft of this audit report. FHFA provided technical comments on the draft report and those comments were considered in finalizing this report. FHFA also provided a management response, which is included in the Appendix of this report. In its management response, FHFA agreed with all of our recommendations and included the following planned corrective actions:

1. FHFA will validate the minimum-security requirements and document their implementation in system specific Customer Controls documents for all existing cloud-based GSS Tools by June 30, 2021, and ensure that any applicable IT security requirements are validated for future cloud-based acquisitions.

2. FHFA will ensure that future cloud-based acquisitions include applicable IT security provisions, and develop and update procedures that include: revised IT security provisions, conditions for including IT security provisions, steps to ensure that OTIM has reviewed applicable pre-award acquisition material, and steps for validating that the IT security provisions are part of the final acquisition package. FHFA will develop the new procedures by April 30, 2021. FHFA also noted that although existing contracts will not be modified, all FHFA's non-compliant GSS Tool contracts will be renewed on or before September 30, 2021, and be subject to the new procedures.

3. OTIM will reinforce the requirements of the IS Characterization Methodology to OTIM Security staff by June 30, 2021.

We consider FHFA's planned corrective actions responsive to our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY ....

We conducted this audit to determine whether FHFA followed its policies for cloud-based IT services. Our review period was April 2018 through April 2020.

To accomplish our objective, we:

- Reviewed the following laws, directives, and guidance applicable to Federal agencies governing the use and security of cloud services for information systems:
  - Public Law 107-437, "The E-Government Act of 2002" Title III, The Federal Information Security Management Act of 2002; as amended by Public Law 113-283, "Federal Information Security Modernization Act of 2014;"
  - White House, Federal Cloud Computing Strategy (Cloud First Policy) (February 2011);
  - OMB memorandum, "Security Authorization of Information Systems in Cloud Computing Environments" (December 2011) and supplementary guidance on the FedRAMP website;
  - OMB Federal Cloud Computing Strategy (Cloud Smart) (June 2019);
  - NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (April 2013, updated January 2015);
  - NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (December 2011); and
  - NIST SP 800-145, The NIST Definition of Cloud Computing (September 2011).
- Reviewed FHFA's Acquisition Policy (June 2011) and Acquisition Procedures Manual, Version 2019.01 (June 26, 2019), Version 2018.01 (April 12, 2018), Version 2017.01 (April 26, 2017), Version 2017.02 (August 8, 2017), Version 2015 (March 3, 2015).
- Reviewed and analyzed FHFA's Cloud Computing Strategy (April 2020), and determined whether that strategy was consistent with OMB's Cloud Smart strategy.
- Reviewed and analyzed the IS Characterization Methodology, approved by FHFA's CIO and Chief Privacy Officer in April 2019, and determined whether FHFA's methodology was consistent with OMB, FedRAMP, and NIST guidance.

- Reviewed and analyzed FHFA’s cloud services inventory provided in April 2020 and reconciled against FHFA’s FISMA system inventory (for FISMA Reportable Information Systems) and FHFA’s GSS inventory (for GSS Tools). Also, determined whether FHFA has documented ATOs to operate cloud services in accordance with the IS Characterization Methodology.

- Determined whether FHFA completed a cloud migration plan, which identified services and data to be migrated.

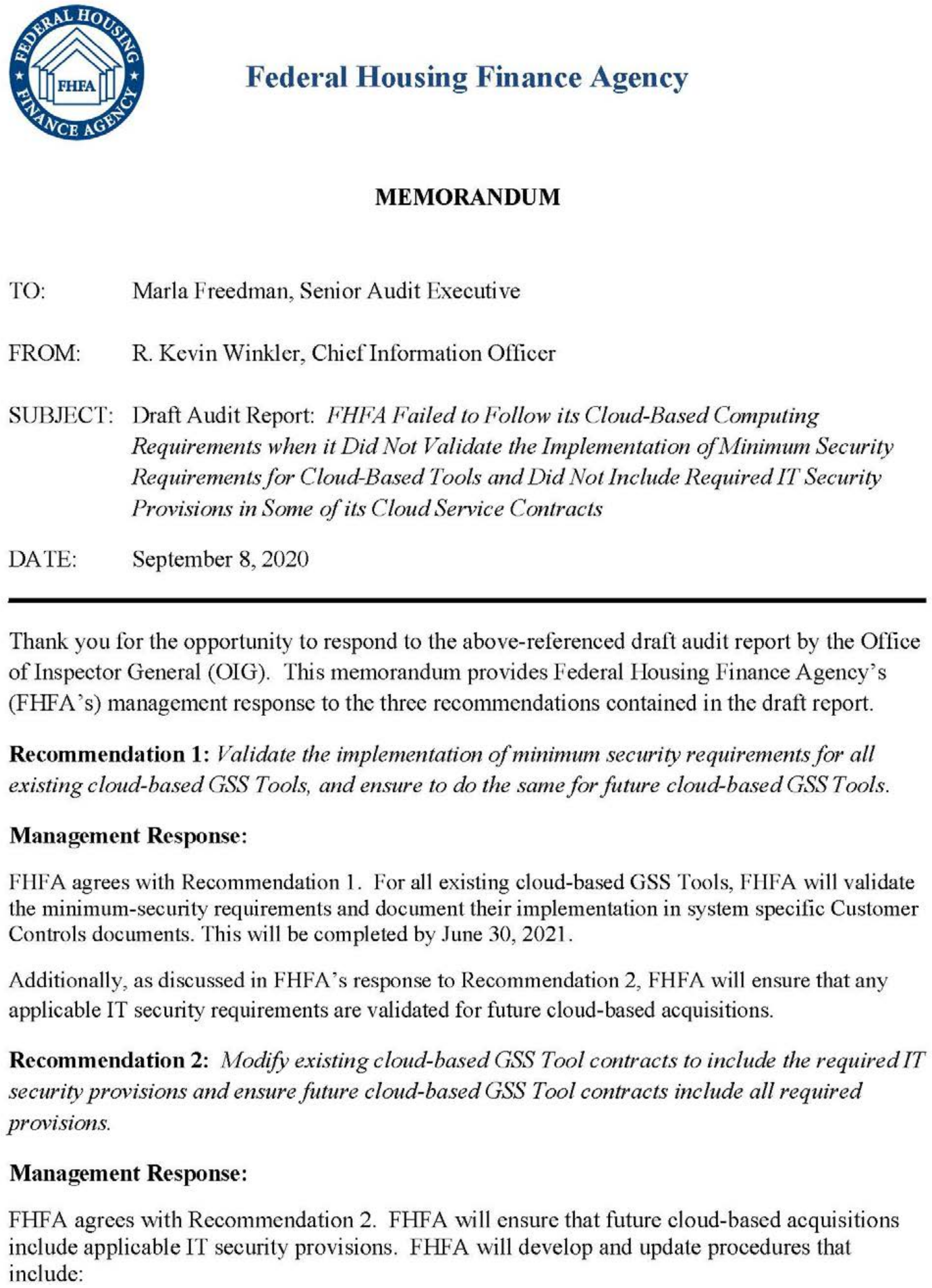
- Determined whether FHFA assessed the risks before migrating data and services onto a cloud provider.

- Reviewed and analyzed contract documents pertaining to FHFA’s acquisition of the 18 cloud services identified by FHFA in April 2020 cloud services inventory and determined whether they contained contract clauses required by FHFA’s Acquisition Procedures Manual and IS Characterization Methodology for IT security and security control verification.

- Interviewed officials and staff of FHFA’s OTIM and OBFM regarding FHFA’s strategy, acquisition, security review, and use of cloud computing services.

We conducted this performance audit between April 2020 and September 2020 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 objective.

APPENDIX: FHFA MANAGEMENT RESPONSE..........................



Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Senior Audit Executive

FROM: R. Kevin Winkler, Chief Information Officer

SUBJECT: Draft Audit Report: *FHFA Failed to Follow its Cloud-Based Computing Requirements when it Did Not Validate the Implementation of Minimum Security Requirements for Cloud-Based Tools and Did Not Include Required IT Security Provisions in Some of its Cloud Service Contracts*

DATE: September 8, 2020

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

Recommendation 1: *Validate the implementation of minimum security requirements for all existing cloud-based GSS Tools, and ensure to do the same for future cloud-based GSS Tools.*

Management Response:

FHFA agrees with Recommendation 1. For all existing cloud-based GSS Tools, FHFA will validate the minimum-security requirements and document their implementation in system specific Customer Controls documents. This will be completed by June 30, 2021.

Additionally, as discussed in FHFA's response to Recommendation 2, FHFA will ensure that any applicable IT security requirements are validated for future cloud-based acquisitions.

Recommendation 2: *Modify existing cloud-based GSS Tool contracts to include the required IT security provisions and ensure future cloud-based GSS Tool contracts include all required provisions.*

Management Response:

FHFA agrees with Recommendation 2. FHFA will ensure that future cloud-based acquisitions include applicable IT security provisions. FHFA will develop and update procedures that include:

- Revised IT security provisions;
- Conditions for including IT security provisions;
- Steps to ensure that OTIM has reviewed applicable pre-award acquisition material; and
- Steps for validating that the IT security provisions as part of the final acquisition package.

FHFA will the develop the new procedures by April 30, 2021.

Although existing contracts will not be modified, all FHFA's non-compliant GSS Tool contracts will be renewed on or before September 30, 2021 and be subject to the new procedures.

Recommendation 3: *Reinforce the requirements in the IS Characterization Methodology to OTIM Security staff.*

Management Response:

FHFA agrees with Recommendation 3. OTIM will reinforce the requirements of the IS Characterization Methodology to OTIM Security staff by June 30, 2021.

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

9/10/2020

X R. Kevin Winkler

R. Kevin Winkler
Chief Infromation Officer
Signed by: ROBERT WINKLER

CC: Chris Bosland
Kate Fulton
Craig Sherman
Ralph Mosios
John Major

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