Federal Housing Finance Agency
Office of Inspector General

Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2024

Audit Report • AUD-2024-006 • July 30, 2024

OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency
400 7th Street SW, Washington, DC 20219

July 30, 2024

TO: Mr. Luis Campudoni, Chief Information Officer

FROM: James Hodge, Deputy Inspector General for Audits /s/

SUBJECT: Audit Report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2024* (AUD-2024-006)

We are pleased to transmit the subject report.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, among other things, to develop, document, and implement agency-wide information security programs and practices to protect information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, federal agencies must undergo an annual independent evaluation of their information security programs and practices.

Pursuant to FISMA, we contracted with CliftonLarsonAllen LLP (CLA), a certified independent public accounting firm, to conduct the fiscal year (FY) 2024 independent evaluation of the Agency's (collectively, the Federal Housing Finance Agency (FHFA) and the FHFA Office of Inspector General (OIG)) information security programs and practices. Effective January 1, 2024, Sikich CPA LLC (Sikich) acquired CLA's federal practice, which included its work for FHFA OIG. Accordingly, Sikich conducted the FISMA evaluation as a performance audit under generally accepted government auditing standards. The objectives of this performance audit were to: (1) evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines; and (2) respond to the FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics. Sikich reviewed selected controls mapped to these metrics for a sample of information systems in the Agency's FISMA inventories of reportable information systems.

Sikich concluded that, while the Agency substantially complied with FISMA and related information security policies and procedures, standards, and guidelines, the Agency's information security programs and practices were not effective. Specifically, the Agency is at an overall Level 3 – *Consistently Implemented* maturity level. Sikich identified 5 new weaknesses in 3 of 5 Cybersecurity Functions and within 3 of the 9 Inspector General FISMA Metric domains. To address these weaknesses, Sikich made 12 new recommendations to assist the

Agency in strengthening its information security programs and practices and noted eight open recommendations from prior audits.

In connection with the contract, we reviewed Sikich's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to conclude, and we do not conclude, on the effectiveness of the Agency's implementation of its information security programs and practices and compliance with FISMA and related information security policies, procedures, standards, and guidelines. Sikich is responsible for the attached auditor's report dated July 30, 2024, and the conclusions expressed therein. Our review found no instances where Sikich did not comply, in all material respects, with generally accepted government auditing standards.

As discussed in the auditor's report, the Agency's management agreed with the recommendations made in the report and outlined its plans to address them.

Attachment

ATTACHMENT

Audit of the Federal Housing Finance Agency's
Information Security Programs and Practices,
Fiscal Year 2024

PERFORMANCE AUDIT OF THE FEDERAL HOUSING FINANCE AGENCY'S INFORMATION SECURITY PROGRAMS AND PRACTICES FOR 2024

SUBMITTED TO THE
FEDERAL HOUSING FINANCE AGENCY
OFFICE OF THE INSPECTOR GENERAL

PERFORMANCE AUDIT REPORT

JULY 22, 2024

FINAL

ACCOUNTING TECHNOLOGY ADVISORY

SIKICH®

333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

SIKICH.COM

July 22, 2024

The Honorable Brian M. Tomney
Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024

Dear Inspector General Tomney:

Sikich CPA LLC (Sikich)[1] is pleased to present our report on the results of our audit of the Federal Housing Finance Agency's (FHFA) and the FHFA Office of Inspector General's (FHFA-OIG) information security programs and practices for the 12 months ending on March 31, 2024, in accordance with the Federal Information Security Modernization Act of 2014. Our report presents the combined results of FHFA and FHFA-OIG (collectively referred to as the Agency). We performed this audit under contract with the FHFA-OIG.

We have reviewed the Agency's responses to a draft of this report and have included our evaluation of management's comments within this final report. The Agency's comments are included in Appendix IV.

We appreciate the assistance we received from the Agency. We will be pleased to discuss any questions you may have regarding the contents of this report.

Sincerely,

Sikich CPA LLC

Alexandria, VA

[1] Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's (CLA's) federal practice, including its work for the Federal Housing Finance Agency Office of Inspector General.

INSPECTOR GENERAL

FEDERAL HOUSING FINANCE AGENCY

Sikich CPA LLC (Sikich) conducted a performance audit of the Federal Housing Finance Agency (FHFA) and FHFA Office of Inspector General's (FHFA-OIG), collectively referred to as the Agency for reporting combined results, information security programs and practices for the 12 months ending on March 31, 2024, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an agency-wide information security program and practices. FISMA also requires Inspectors General (IG) to conduct an annual independent evaluation of their agencies' information security programs and practices.

The objectives of this performance audit were: (1) to evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines, and (2) to respond to the fiscal year (FY) *2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2024 IG FISMA Reporting Metrics).

We conducted this performance audit 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.

For this year's review, IGs were required to assess 20 core and 17 supplemental IG FISMA Reporting Metrics across 5 security function areas—Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agencies' information security programs and the maturity level of each function area.[2] The maturity levels are Level 1 – *Ad Hoc*, Level 2 – *Defined*, Level 3 – *Consistently Implemented*, Level 4 – *Managed and Measurable*, and Level 5 – *Optimized*. To be considered effective, an agency's information security program must be rated Level 4 – *Managed and Measurable*.

The audit included an assessment of the Agency's information security programs and practices consistent with FISMA and reporting instructions issued by the Office of Management and Budget (OMB). The scope also included assessing selected controls outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the FY 2024 IG FISMA Reporting Metrics, for a sample of systems in the Agency's FISMA inventories of information systems.

[2] The function areas are further broken down into nine domains (Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning).

The scope of this performance audit included the Agency's information security programs and practices covering the period from April 1, 2023, through March 31, 2024. We conducted audit fieldwork from October 2023 through June 2024.

We concluded that the Agency substantially complied with FISMA and related information security policies and procedures, standards, and guidelines. While the Agency substantially complied with FISMA, we concluded that the Agency's information security programs and practices were not effective. Specifically, the Agency is at an overall Level 3 – *Consistently Implemented* maturity level. We identified 5 new weaknesses in 3 of 5 Cybersecurity Functions, and within 3 of the 9 IG FISMA Metric domains. As a result, we made 12 new recommendations to assist the Agency in strengthening its information security programs and practices.

Further, there were weaknesses from FHFA-OIG audits and open prior year FISMA recommendations that impacted the IG FISMA Reporting metrics, in the Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Incident Response, and Contingency Planning domains. As such, eight recommendations related to prior FISMA audits are still open.

Additional information on our findings and recommendations is included in the accompanying report.

Sikich CPA LLC

Alexandria, VA
July 22, 2024

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also requires agency Inspectors General (IGs) to assess the effectiveness of their agency's information security program and practices. The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

The Federal Housing Finance Agency Office of Inspector General (FHFA-OIG) engaged Sikich CPA LLC (Sikich)[3] to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of FHFA's and FHFA-OIG's (collectively referred to as the Agency for reporting combined results) information security programs and practices. The objectives of this performance audit were: (1) to evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines, and (2) to respond to the fiscal year (FY) *2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2024 IG FISMA Reporting Metrics).[4]

The scope of this performance audit included the Agency's information security programs and practices covering the period from April 1, 2023, through March 31, 2024. We conducted audit fieldwork from October 2023 through June 2024.

The FY 2024 IG FISMA Reporting Metrics require us to assess the maturity of five functional areas in the Agency's information security programs and practices. For this year's review, IGs were required to assess 20 core[5] and 17 supplemental[6] IG FISMA Reporting Metrics across five security function areas—Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agencies' information security program and the maturity level of each function area.[7] The maturity levels are Level 1 – *Ad Hoc*, Level 2 – *Defined*, Level 3 – *Consistently Implemented*, Level 4 – *Managed and Measurable*, and Level 5 – *Optimized*. To be considered effective, an agency's information security program must be rated Level 4 – *Managed and Measurable*. See Appendix I for additional information on the FY 2024 IG FISMA Reporting Metrics and FISMA reporting requirements.

For this audit, Sikich reviewed selected controls outlined in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*,

[3] See Footnote 1.

[4] See the FY 2024 IG FISMA Reporting Metrics online here.

[5] Core metrics are assessed annually and represent a combination of Administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.

[6] Supplemental metrics are assessed at least once every 2 years. They represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

[7] The function areas are further broken down into nine domains.

supporting the FY 2024 IG FISMA Reporting Metrics, for a sample of information systems[8] in the Agency's FISMA inventories of information systems.

We conducted this performance audit 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.

II. AUDIT RESULTS

Progress Since 2023

At the beginning of our performance audit, there were 17 open recommendations from prior FISMA and Privacy audits (1 open recommendation from the FY 2020 FISMA audit,[9] 1 open recommendation from the FY 2021 Privacy audit,[10] 10 open recommendations from the FY 2023 FISMA audit,[11] and 5 open recommendations from the FY 2023 Privacy audit).[12] During the audit, we found that the Agency took corrective actions to address nine recommendations, and we consider those recommendations closed. Corrective actions are in progress on the other eight open recommendations. Refer to Appendix III for a detailed description of the status of each recommendation.

Current Status

We concluded that the Agency substantially complied with FISMA and related information security policies and procedures, standards, and guidelines. While the Agency substantially complied with FISMA, we concluded that the Agency's information security programs and practices were not effective. Specifically, we noted that two Cybersecurity Framework functions achieved a maturity level of Level 3 – *Consistently Implemented*, two achieved a maturity level of Level 4 – *Managed and Measurable,* and one achieved a maturity level of Level 2 – *Defined*. As a result, the Agency's overall maturity level was rated as Level 3 – *Consistently Implemented* (Not Effective).[13] **Table 1** on the following page shows a summary of the overall maturity levels for each security function and domain in the FY 2024 IG FISMA Reporting Metrics.

[8] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[9] FHFA-OIG Audit Report AUD-2021-001, *Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2020* (October 20, 2020).

[10] FHFA-OIG Audit Report AUD-2021-011, *Audit of the Federal Housing Finance Agency's 2021 Privacy Program* (August 11, 2021).

[11] FHFA-OIG Audit Report AUD-2023-004, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2023* (July 26, 2023).

[12] FHFA-OIG Audit Report 2023-006, *Audit of the Federal Housing Finance Agency's Privacy Program Fiscal Year 2023* (August 23, 2023).

[13] The FY 2024 IG FISMA Reporting Metrics were provided as a separate deliverable. The FY 2024 IG FISMA Reporting Metrics deliverable included calculated average scores for the FY 2024 core and supplemental IG FISMA Reporting Metrics.

Table 1: Maturity Levels for FY 2024 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions[14]	Maturity Level by Function	Domain	Maturity Level by Domain
Identify	Level 3: Consistently Implemented (Not Effective)	Risk Management	Level 4: Managed and Measurable (Effective)
		Supply Chain Risk Management	Level 2: Defined (Not Effective)
Protect	Level 3: Consistently Implemented (Not Effective)	Configuration Management	Level 3: Consistently Implemented (Not Effective)
		Identity and Access Management	Level 2: Defined (Not Effective)
		Data Protection and Privacy	Level 3: Consistently Implemented (Not Effective)
		Security Training	Level 5: Optimized (Effective)
Detect	Level 4: Managed and Measurable (Effective)	Information Security Continuous Monitoring	Level 4: Managed and Measurable (Effective)
Respond	Level 4: Managed and Measurable (Effective)	Incident Response	Level 4: Managed and Measurable (Effective)
Recover	Level 2: Defined (Not Effective)	Contingency Planning	Level 2: Defined (Not Effective)
Overall	**Level 3: Consistently Implemented (Not Effective)**		

Source: Sikich's analysis of the Agency's maturity levels for the FY 2024 IG FISMA Reporting Metrics.

In accordance with the FY 2024 IG FISMA Reporting Metrics guidance,[15] we focused on the calculated average scores of the core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average scores of the supplemental IG FISMA Reporting Metrics, progress made in addressing outstanding prior-year FISMA audit recommendations, and other data sources (e.g., FHFA-OIG audits) to come to this risk-based conclusion. As a result, the Agency's overall maturity level was rated as Level 3 – *Consistently Implemented* (Not Effective).

The new weaknesses we identified during this audit, in combination with prior-year open recommendations and weaknesses noted in FHFA-OIG's audits,[16] significantly impacted the Agency's overall information security programs and practices. Specifically, the Agency needs to improve controls over Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, and Contingency Planning. See **Table 2** below for a mapping of weaknesses to IG FISMA Reporting Metrics

[14] See Appendix I, Tables 3 and 4, for definitions and explanations of the Cybersecurity Framework security functions and domains and maturity levels, respectively.

[15] The FY 2024 IG FISMA Reporting Metrics provided the agency IG the discretion to determine the rating for each of the Cybersecurity Framework domains and functions and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FISMA audit. Using this approach, IGs may determine that a particular domain, function area, or agency's information security program is effective at a calculated maturity lower than Level 4.

[16] The following audits that impacted the IG FISMA Reporting Metrics were taken into consideration: FHFA-OIG, *FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines* (March 8, 2023) (AUD-2023-002), and FHFA-OIG's ongoing internal penetration test audit of FHFA's network and systems (Assignment No. OA-24-005).

domains. These key weaknesses need to be addressed in a comprehensive manner to achieve an effective rating of Level 4 – *Managed and Measurable*.

We identified five new weaknesses in the Identity and Access Management, Information Security Continuous Monitoring, and Contingency Planning domains of the FY 2024 IG FISMA Reporting Metrics (see Findings 1 through 5 in **Table 2**). As such, we made 12 new recommendations to assist the Agency in strengthening its information security programs and practices. **Table 2** also includes weaknesses where the Agency has eight prior-year recommendations that remain open (refer to **Appendix III**) and weaknesses from FHFA-OIG audits that impact the IG FISMA Reporting Metrics. The weaknesses from FHFA-OIG audits are included in this report by reference only.

In combination, these control weaknesses affect the Agency's ability to preserve the confidentiality, integrity, and availability of its information and information systems, potentially exposing it to unauthorized access, use, disclosure, modification, or destruction.

Table 2: Weaknesses Noted in FY 2024 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2024 IG FISMA Reporting Metrics

Cybersecurity Framework Security Function	IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	Risk Management	FHFA-OIG's ongoing internal penetration test of FHFA's network and systems revealed Office of Technology and Information Management's (OTIM's) shortcomings related to software management controls.
	Supply Chain Risk Management	Open prior-year recommendations related to developing a process to communicate relevant secure software development requirements to vendors.
Protect	Configuration Management	Open prior-year recommendations related to remediating vulnerabilities in a timely manner. FHFA-OIG's ongoing internal penetration test of FHFA's network and systems revealed OTIM's shortcomings related to configuration management controls.
	Identity and Access Management	Open prior-year recommendation related to implementing planned multi-factor authentication for privileged accounts for internal systems. Open prior-year recommendations related to event logging (EL) maturity. Weaknesses Identified in FHFA's Background Reinvestigations Process (**Finding 1**). Weaknesses Identified in FHFA-OIG's Background Reinvestigations Process (**Finding 2**). Weaknesses Identified in FHFA's Management of a Cloud System's User Accounts (**Finding 3**). FHFA-OIG's ongoing internal penetration test of FHFA's network and systems revealed OTIM's shortcomings related to access controls.

Cybersecurity Framework Security Function	IG FISMA Reporting Metrics Domain	Weaknesses Noted
	Data Protection and Privacy	FHFA-OIG's ongoing internal penetration test of FHFA's network and systems revealed OTIM's shortcomings related to data protection and privacy controls. FHFA-OIG's 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* (March 8, 2023) (AUD-2023-002), revealed OTIM's shortcomings related to encryption of data at rest.
	Security Training	No weaknesses noted.
Detect	Information Security Continuous Monitoring	FHFA's System Security and Privacy Plans (SSPP) were not reviewed annually (**Finding 4**).
Respond	Incident Response	Open prior-year recommendations related to EL maturity.
Recover	Contingency Planning	Open prior-year recommendation related to the updating of *Disaster Recovery Procedures* to include all necessary components. An FHFA Information System Contingency Plan (ISCP) was not consistently reviewed, updated, and tested annually (**Finding 5**).

Source: Sikich's analysis of the Agency's weaknesses identified during this year's FISMA audit, open prior-year recommendations, and FHFA-OIG audits, mapped back to the IG FISMA Reporting Metrics.

The following section provides a detailed discussion of the audit findings. Appendix I provides background information on FISMA. Appendix II describes the audit objectives, scope, and methodology. Appendix III provides the status of prior-year recommendations. Appendix IV includes the Agency's comments.

III. AUDIT FINDINGS

1. Weaknesses Identified in FHFA's Background Reinvestigations Process

Cybersecurity Framework Security Function: *Protect*

FY 2024 IG FISMA Reporting Metrics Domain: *Identity and Access Management*

The following issues were identified related to FHFA's background reinvestigations policies and procedures and the timeliness of background reinvestigations.

Background Reinvestigation Policies and Procedures

FHFA did not develop policies and procedures to oversee FHFA's service provider[17] and the tracking of the reinvestigation process.

Background Reinvestigation Timeliness

Based on a review of the FHFA background investigation spreadsheet[18] as of February 28, 2024, we found that 59 of 1,166[19] individuals[20] had overdue background reinvestigations. Specifically, we found the following individuals' background reinvestigations (broken down by background investigation tier) were overdue:

- **Tier 2:**[21] Out of 492 individuals (305 employees and 187 contractors), 47 (18 employees and 29 contractors) had neither enrolled in Trusted Workforce (TW)[22] nor undergone a background reinvestigation within the past 5 years, as the Office of Personnel Management (OPM) requires.

[17] FHFA's service provider provides personnel security services to FHFA and other United States federal agencies and is part of an executive department of the United States federal government. Under the service level agreement between FHFA and its service provider, the service provider is responsible for tracking the investigative status of all FHFA federal and contract employees to determine when they are due for reinvestigations.

[18] This spreadsheet was provided by FHFA's service provider, and it details employees' and contractors' background investigation statuses. It includes several fields (e.g., name, position sensitivity levels, position titles, investigation type, date investigation closed).

[19] The 1,166 individuals consisted of 764 FHFA employees and 402 FHFA contractors.

[20] According to the FHFA background investigation spreadsheet, dated February 28, 2024, 563 individuals underwent timely background reinvestigations for Tier 1 investigations, and 2 individuals did so for Tier 3 investigations. A Tier 1 investigation is the lowest level of background check by the federal government, suitable for non-sensitive positions that pose a low risk. The Defense Counterintelligence and Security Agency Position Designation Investigation Chart from September 2017 states that there is no need for reinvestigations in low-risk Tier 1 positions. A Tier 3 investigation applies to moderate-risk, non-critical sensitive national security positions, qualifying an individual for a Secret clearance.

[21] A Tier 2 investigation applies to moderate-risk positions in non-sensitive public trust roles. Public trust positions require a certain level of eligibility to access sensitive information.

[22] Enrollment in the TW system means that an individual will undergo continuous vetting (CV) instead of periodic reinvestigations. CV involves regular reviews of a cleared individual's background to confirm they will still meet the requirements for their security clearance continuation in positions of trust. This process includes automated record checks that pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's eligibility. CV helps address personnel security issues proactively by mitigating potential risks or, in some instances, suspending or revoking clearances if necessary.

- **Tier 4:**[23] Out of 91 individuals (85 employees and 6 contractors), 11 (9 employees and 2 contractors) had neither enrolled in TW nor undergone a background reinvestigation within the past 5 years, as OPM requires.
- **Tier 5:**[24] Out of 18 individuals (17 employees and 1 contractor), 1 employee had neither enrolled in TW nor undergone a background reinvestigation within the past 5 years, as OPM requires.

The FHFA Associate Director for Agency Operations stated that the Office of Facilities and Operations Management (OFOM) did not develop policies and procedures related to FHFA's reinvestigation process because it was relying on its service provider to perform the reinvestigation process. FHFA was in the process of developing policies and procedures related to background reinvestigations.

Additionally, the FHFA Associate Director for Agency Operations stated that FHFA did not have policies and procedures established to monitor or provide oversight of its service provider. Specifically, the service level agreement between FHFA and the service provider did not include requirements for the service provider to provide background reinvestigation status reports on a regular basis. Therefore, the service provider did not inform FHFA when a federal employee or a contractor was due for a reinvestigation or when the reinvestigation process was initiated.

Further, the FHFA Associate Director for Agency Operations stated that TW will ultimately replace the need for existing legacy reinvestigation models. It was intended that TW would replace the legacy models at the beginning of FY 2024. However, the TW implementation was delayed and caused employees' and contractors' background investigations to expire and become overdue. FHFA's Personnel Security will coordinate with the service provider and determine if FHFA will continue to await TW deployment or initiate reinvestigations.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (December 10, 2020), security control Personnel Security (PS)-1 (Policy and Procedures), requires organizations to develop and document a personnel security policy and procedures to facilitate the implementation of personnel security policy and controls.

NIST SP 800-53, Revision 5, security control PS-3 (Personnel Screening), requires that an organization rescreen individuals according to an organization-defined frequency. Additionally,

FHFA Personnel Security Standard (November 30, 2022), Section 2, requires that FHFA adhere to OPM guidance for the screening and rescreening of individuals.

[23] A Tier 4 investigation is designated for high-risk positions within non-sensitive public trust areas.

[24] A Tier 5 investigation is used for high-risk national security positions that require critical sensitivity. It qualifies an individual for a Top Secret clearance.

Tier 2 and Tier 4 Criteria

OPM's regulation at Title 5 Code of Federal Regulations (CFR), Part 731.106, requires agencies to submit and adjudicate public trust[25] reinvestigations at least once every 5 years.

OPM Memorandum, *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Continuous Vetting for Non-Sensitive Public Trust Positions* (March 8, 2024), requires the following:

- Agencies must enroll employees and contractors in non-sensitive public trust positions into TW by 2024 or conduct a reinvestigation.
- Individuals in non-sensitive public trust positions must have completed an investigative form within the last 5 years. The investigative form contains the necessary consent for enrollment into TW.
- Enrollment of non-sensitive public trust personnel into TW will replace the requirement for periodic reinvestigations. If the background investigation form was completed more than 5 years ago, the Department must collect a new investigative form.

Tier 3 and Tier 5 Criteria

OPM Memorandum, *Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0* (January 15, 2021), required that individuals occupying national security positions (Tier 3 and Tier 5) be enrolled in TW by September 30, 2022.

Due to the lack of background reinvestigation policies and procedures, OFOM did not effectively oversee FHFA's service provider, and that has contributed to FHFA's lack of a process to track the reinvestigation process.

Without effective tracking of background reinvestigation data for employees and contractors, there is a risk that they will not be reinvestigated timely, as demonstrated above. Therefore, FHFA is at risk of allowing unnecessary or unauthorized access to sensitive systems and data for individuals that were not reinvestigated for their job responsibilities.

We recommend that the FHFA Chief Information Officer, in coordination with the Associate Director for Agency Operations:

- **Recommendation 1:** Develop and implement policies and procedures to oversee FHFA's background reinvestigation process, including oversight controls over FHFA's service provider.
- **Recommendation 2:** Update the service level agreement between FHFA and the service provider to include requirements for the service provider to provide background reinvestigation status reports on a regular basis.
- **Recommendation 3:** Implement a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance with FHFA and OPM standards.

[25] Public trust signifies a specific level of eligibility to access sensitive information.

2. Weaknesses Identified in FHFA-OIG's Background Reinvestigations Process

Cybersecurity Framework Security Function: *Protect*

FY 2024 IG FISMA Reporting Metrics Domain: *Identity and Access Management*

The following issues were identified related to FHFA-OIG's background reinvestigations policies and procedures, the timeliness of background reinvestigations, and adjudication determinations.

Background Reinvestigation Policies and Procedures

FHFA-OIG did not develop policies and procedures to oversee FHFA-OIG's service provider[26] and the tracking of the reinvestigation process.

Reinvestigation Timeliness

Based on a review of FHFA-OIG's background investigation spreadsheet[27] as of December 19, 2023, we found that 5 of 144[28] FHFA-OIG individuals[29] had overdue background reinvestigations. Specifically, we found the following individuals' background reinvestigations (broken down by background investigation tier) were overdue:

- **Tier 2:**[30] Out of the 91 individuals (65 employees and 26 contractors), 4 (2 employees and 2 contractors) had neither enrolled in TW[31] nor undergone a background reinvestigation within the past 5 years, as OPM requires.
- **Tier 4:**[32] Out of three employees, one had neither enrolled in TW nor undergone a background reinvestigation within the past 5 years, as OPM requires.

[26] FHFA-OIG's service provider provides personnel security services to FHFA-OIG and other United States federal agencies and is part of an executive department of the United States federal government. Under the service level agreement between FHFA-OIG and its service provider, the service provider is responsible for tracking the investigative status of all FHFA-OIG federal and contract employees to determine when they are due for reinvestigations.

[27] This spreadsheet was provided by FHFA-OIG's service provider and details employees' and contractors' background investigation status. It includes several fields (e.g., name, required position sensitivity levels, position titles, investigation type, investigation completion date).

[28] The 144 individuals consisted of 119 FHFA-OIG employees and 25 FHFA-OIG contractors.

[29] According to the FHFA-OIG background investigation spreadsheet, dated December 19, 2023, 2 individuals underwent timely background reinvestigations for Tier 3 investigations and 48 individuals underwent timely background reinvestigations for Tier 5 investigations. There were no individuals with Tier 1 investigations. A Tier 1 investigation is the lowest level of background check by the federal government, suitable for non-sensitive positions that pose a low risk. The Defense Counterintelligence and Security Agency, Position Designation Investigation Chart from September 2017 states that there is no need for reinvestigations in low-risk Tier 1 positions. A Tier 3 investigation applies to moderate-risk, non-critical sensitive national security positions, qualifying an individual for a Secret clearance. A Tier 5 investigation is used for high-risk national security positions that require critical sensitivity. It qualifies an individual for a Top Secret clearance.

[30] See Footnote 21.

[31] See Footnote 22.

[32] See Footnote 23.

Adjudication Determinations

FHFA-OIG delegated the duties of conducting suitability adjudicative determinations and executing related actions for covered[33] positions to its service provider. Suitability determinations assess individuals' character traits and conduct to decide whether they are fit for specific roles. Actions based on these determinations can include cancellation of eligibility, removal, cancellation of reinstatement of eligibility, and debarment. FHFA-OIG's delegation of duties to its service provider did not comply with OPM's requirements.

The FHFA-OIG Director of Human Resources stated that the Human Resources Division (HRD) did not develop policies and procedures related to FHFA-OIG's reinvestigation process because it was relying on its service provider to perform the reinvestigation process. Additionally, the FHFA-OIG Director of Human Resources stated that FHFA-OIG did not have policies and procedures established to monitor or provide oversight of its service provider. Specifically, the service level agreement between FHFA-OIG and the service provider did not include requirements for the service provider to provide background reinvestigation status reports on a regular basis. Therefore, the service provider did not inform FHFA-OIG when a federal employee or a contractor was due for a reinvestigation or when the reinvestigation process was initiated.

In addition, the FHFA-OIG Director of Human Resources stated that TW will ultimately replace the need for existing legacy reinvestigations models. It was intended that TW would replace legacy models at the beginning of the FY 2024. However, the TW implementation was delayed, which caused employee and contractor background reinvestigations to expire and become overdue. HRD will coordinate with the service provider and determine if FHFA-OIG will continue to await TW deployment or initiate reinvestigations.

Further, in relation to adjudications, the FHFA-OIG Director of Human Resources stated FHFA-OIG was unaware that it could not delegate this responsibility to its service provider. The service provider reported that, based on a recent audit with one of its other customer agencies, it was in the process of introducing a new business model that will allow FHFA-OIG to make adjudication decisions. The service provider scheduled an educational forum for May 2024, where it introduced this strategy to its customers. FHFA-OIG Human Resources and other administrative staff registered to attend the educational forum.

NIST SP 800-53, Revision 5, security control PS-1, requires organizations to develop and document a personnel security policy and procedures to facilitate the implementation of personnel security policy and controls. Additionally, NIST SP 800-53, Revision 5, security control PS-3, requires that an organization rescreen individuals according to an organization-defined frequency.

FHFA-OIG's *General Support System (OIGNet) System Security Plan (SSP) & Control Implementation Procedures* (May 4, 2023), security control PS-3, states that FHFA-OIG relies on OPM guidance for determining re-screening criteria and timetables, as well as conducting the re-screening.

[33] Pursuant to 5 CFR 731.101(b), a "covered position" means a position in the competitive service, a position in the excepted service that can non-competitively convert to the competitive service, or a career appointment to a position in the Senior Executive Service.

Tier 2 and Tier 4 Criteria

OPM's regulation under Title 5 CFR, Part 731.106, requires agencies to submit and adjudicate public trust reinvestigations at least once every 5 years.

OPM Memorandum, *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Continuous Vetting for Non-Sensitive Public Trust Positions* (March 8, 2024), requires the following:

- Agencies must enroll employees and contractors in non-sensitive public trust positions into TW.
- Individuals in non-sensitive public trust positions must have completed an investigative form within the last 5 years. The investigative form contains the necessary consent for enrollment into TW.
- Enrollment of non-sensitive public trust personnel into TW will replace the requirement for periodic reinvestigations. If the background investigation forms were completed more than 5 years ago, the Department must collect a new investigative form.

Adjudication Determination Criteria

OPM's regulation under Title 5 CFR, Part 731.103, states that "OPM delegates to the heads of agencies' authority for making suitability determinations and taking suitability actions."

Due to the lack of background reinvestigation policies and procedures, HRD did not effectively oversee FHFA-OIG's service provider, which has contributed to FHFA-OIG's lack of a process to track the reinvestigation process.

Without effective tracking of background reinvestigation data for employees and contractors, there is a risk that they will not be reinvestigated timely, as demonstrated above. Therefore, FHFA-OIG is at risk of allowing unnecessary or unauthorized access to sensitive systems and data for individuals that were not reinvestigated for their job responsibilities.

Not following OPM's regulation as outlined in Title 5 CFR, Part 731.103, related to the adjudication process, negatively impacts FHFA-OIG's ability to effectively execute its delegated responsibilities. Because the service provider is a separate entity from FHFA-OIG, it may not have direct knowledge about the positions and individuals to best assess suitability adjudications for individuals.

We recommend that FHFA-OIG's Chief Information Officer, in coordination with the Director of Human Resources:

- **Recommendation 4:** Develop and implement policies and procedures to oversee FHFA-OIG's background reinvestigation process, including oversight controls over FHFA-OIG's service provider.
- **Recommendation 5:** Update the service level agreement between FHFA-OIG and the service provider to include requirements for the service provider to provide background reinvestigation status reports on a regular basis.
- **Recommendation 6:** Implement a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance with FHFA-OIG and OPM standards.

- **Recommendation 7:** Establish and implement a process to make suitability adjudicative determinations and take suitability actions for covered positions in accordance with OPM's regulation under Title 5 CFR, Part 731.103.

3. Weaknesses Identified in FHFA's Management of a Cloud System's User Accounts

Cybersecurity Framework Security Function: *Protect*

FY 2024 IG FISMA Reporting Metrics Domain: *Identity and Access Management*

Based on our review of a cloud system's[34] user account listing as of January 25, 2024, we found that 20 from a total of 588[35] users (3.4 percent) had not accessed their accounts in more than a year, yet these accounts were still active. Further, we found that there was not a process in place to periodically review the cloud system's non-privileged users' access.

An FHFA OTIM Senior Information Technology (IT) Specialist stated that, on August 1, 2022, the cloud system encountered a control functions failure due to vendor software glitches. The root cause of this failure was traced back to a Federal Risk and Authorization Management Program (FedRAMP)[36]-approved third-party encryption software that FHFA had integrated into the system. These software glitches inadvertently allowed 20 of the cloud system's users to remain active beyond the expected 365-day inactivity period.

Additionally, the same OTIM Senior IT Specialist stated that FHFA was not regularly reviewing non-privileged users' access because there was not a specified requirement detailed in the FHFA customer controls for the cloud system.[37] This document only requires that privileged users' access is reviewed periodically.

NIST SP 800-53, Revision 5, security control Access Control (AC)-2, enhancement 3 (Account Management, Disable Accounts), requires that organizations disable accounts when the accounts have been inactive for an organizationally defined time period. Additionally, FHFA customer controls for the cloud system (August 1, 2022) require that accounts be disabled after an inactivity threshold of 365 days.

NIST SP 800-53, Revision 5, security control AC-6, enhancement 7 (Least Privilege, Review of User Privileges), requires that, on an organizationally defined basis, organizations review the access privileges assigned to users to validate the need for such privileges.

As a result of not disabling inactive non-privileged user accounts and the lack of compliance with FHFA customer controls for the cloud system's requirements for a periodic review process for non-privileged users' access, FHFA may risk unauthorized access to the cloud system. This

---

[34] A cloud-based system that provides a secure software as a service (SaaS) solution for government agencies to make the most of the organizations' collective knowledge. The software platform allows agencies to involve the opinions of public and private communities by collecting their ideas and giving users a platform to vote. The cloud system's Privacy Impact Assessment states that the system contains information such as employee names, email addresses, usernames, and zip codes.

[35] The cloud system's user accounts consisted of 3 privileged and 585 non-privileged users.

[36] FedRAMP is a United States federal government-wide compliance program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

[37] Customer Control Plans serve in place of SSPPs to define FHFA's control responsibilities as the customer for systems provided by a third party.

may increase the risk of unauthorized access to sensitive information (e.g., employee names, email addresses, usernames, and zip codes) that can be collected in the cloud system.

We recommend that FHFA's Chief Information Officer:

- **Recommendation 8:** Disable accounts of non-privileged users who have been inactive for over 365 days, as required by the FHFA customer controls for the cloud system.
- **Recommendation 9:** Work with the cloud system's vendor to implement software updates that automatically disable user accounts after 365 days of inactivity, as required by the FHFA customer controls for the cloud system.
- **Recommendation 10:** Update the customer controls for the cloud system to include a procedure for regular reviews of non-privileged users' access.

4. FHFA's System Security and Privacy Plans Were Not Reviewed Annually

Cybersecurity Framework Security Function: *Detect*

FY 2024 IG FISMA Reporting Metrics Domain: *Information Security Continuous Monitoring*

For the following two of four systems selected for testing, FHFA did not review and update the SSPPs or Customer Control Plans on an annual basis:

- A cloud system[38] – *Customer Controls for a Cloud System* (August 1, 2022)
- Capital Models (PolyPaths)[39] – *System Security Plan for PolyPaths* (July 15, 2020)

An OTIM Senior IT Specialist stated that OTIM previously identified this issue within Plan of Action & Milestones (POA&M)[40] ID: Common Control Plan (CCP)-Q4-2022-008 (January 2, 2024) and CCP-Q4-2023-003 (November 27, 2023). These POA&Ms[41] stated that FHFA did not review and update SSPPs or Customer Control Plans on an annual basis due to resource constraints. Specifically, FHFA did not have sufficient Information System Security Officer (ISSO) resources to perform SSPP or Customer Control Plan updates on a timely basis.

Further, the OTIM Senior IT Specialist also stated that FHFA was in the process of hiring additional ISSO resources, with an ISSO scheduled to begin work on April 22, 2024.

---

[38] See Footnote 34.

[39] Capital Models (PolyPaths) is a pricing and risk measurement system used by FHFA financial analysts and economists. It is designed to perform pre-trade analyses, hedging, pricing, and advanced risk analyses on a wide variety of fixed-income instruments, including mortgages and structured products, bonds, derivatives, and credit entrustments, such as corporate and asset-backed credit default swaps.

[40] POA&Ms are management tools that describe the actions that are planned to correct information system security and privacy weaknesses in controls identified during audits, assessments of controls, or continuous monitoring activities. POA&Ms 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&Ms 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.

[41] At the time of testing, these POA&Ms' scheduled completion dates were not past due; specifically, CCP-Q4-2022-008 was extended to June 28, 2024, and CCP-Q4-2023-003's estimated completion date is September 30, 2024.

NIST SP 800-53, security control Planning (PL)-2 (System Security and Privacy Plans), requires that SSPPs be reviewed based upon an organizationally defined frequency. Further, it requires that SSPPs be updated to address changes to the system and environment of operation or problems identified during plan implementation or control assessments.

FHFA's *Planning Standard*, Revision 2.1 (November 30, 2022), states that the SSPP or Customer Control Plans shall be reviewed at least annually and updated as needed. In addition, FHFA's *Common Control Plan* (May 10, 2023), security control PL-2, requires that SSPPs be reviewed annually.

SSPPs and Customer Control Plans are used in FHFA's Assessment and Authorization process to select and document security and privacy controls. Without consistently reviewing and updating SSPPs and Customer Control Plans, the Authorizing Official and other agency stakeholders may not account for security and privacy risks to the systems during the Assessment and Authorization process, potentially impacting the overall risk exposure for FHFA.

Further, inaccurate SSPPs and Customer Control Plans increase the risk that sensitive information contained in these systems is not properly safeguarded. For example, sensitive information (e.g., employee names, email addresses, usernames, zip codes) may be collected in the cloud system.

We recommend that FHFA's Chief Information Officer:

- **Recommendation 11:** Complete the review and update of overdue SSPPs and Customer Control Plans in accordance with the existing related POA&Ms.

5. An FHFA Information System Contingency Plan Was Not Consistently Reviewed, Updated, and Tested Annually

Cybersecurity Framework Security Function: *Recover*

FY 2024 IG FISMA Reporting Metrics Domain: *Contingency Planning*

For one of four systems selected for testing, FHFA did not follow its *Contingency Planning Standard*, Revision 2.1 (November 30, 2022). Specifically, we noted the following:

- The Capital Models (PolyPaths)[42] Information System Contingency Plan (ISCP) had not been reviewed and updated on an annual basis since June 21, 2018.
- The Capital Models (PolyPaths) ISCP had not been tested on an annual basis since the last ISCP update on June 21, 2018.

An OTIM Senior IT Specialist stated that the OTIM previously identified this issue within POA&M[43] ID: Capital Models (PolyPaths) (CMP)-Q4-2021-001 (March 18, 2024). The POA&M[44] stated that FHFA did not review, update, or test the Capital Models (PolyPaths) ISCP on an annual basis due to resource constraints. Specifically, the OTIM Senior IT Specialist stated that

[42] See Footnote 39.

[43] See Footnote 40.

[44] At the time of testing, the POA&M's scheduled completion date was not past due; specifically, CMP-2021-001 was extended until September 30, 2024.

FHFA did not have sufficient ISSO resources to perform updates and testing of the Capital Models (PolyPaths) ISCP. Further, the OTIM Senior IT Specialist stated that FHFA was in the process of hiring additional ISSO resources, with an ISSO who started on April 22, 2024.

NIST SP 800-53, Revision 5, security control CP-2 (Contingency Plan), requires that ISCPs be reviewed at an organizationally defined frequency. Further, ISCPs are updated to address changes to the organization, system, or environment of operations and problems encountered during the ISCP implementation, execution, or testing. In addition, NIST SP 800-53, Revision 5, security control CP-4 (Contingency Plan Testing), requires that ISCPs be tested at an organizationally defined frequency using organizationally defined tests to determine the effectiveness of the plan and the readiness to execute the plan.

FHFA's *Contingency Planning Standard*, Revision 2.1 (November 30, 2022), requires the following:

- Contingency plans shall be reviewed and updated at least annually or at any time in which a change to the operating environment or significant change to recovery procedures has occurred.
- FHFA shall test the contingency plans at least annually, using tabletop exercises and/or functional exercises to determine the effectiveness of the plans and the organizational readiness to execute the plans.

The lack of an annual review and testing of the Capital Models (PolyPaths) ISCP increases the risk that OTIM may not recover the system successfully or timely during a disruption.

We recommend that FHFA's Chief Information Officer:

- **Recommendation 12:** Complete the review, update, and testing of the Capital Models (PolyPaths) ISCP in accordance with the existing related POA&M.

IV. Evaluation of Managements' Comments

In response to a draft of this report, FHFA and FHFA-OIG provided separate management responses related to their specific program's findings and recommendations. FHFA and FHFA-OIG management fully agreed with 11 recommendations and partially agreed with 1 recommendation in this report, and they outlined their plans to address each recommendation. Appendix IV includes the Agency's comments.

FHFA Response

For Recommendation 1, FHFA management agreed with this recommendation. FHFA management stated that OFOM will develop and implement policies and procedures to oversee the Agency's background reinvestigation process, including oversight controls over FHFA's service provider. FHFA expects this action to be completed by December 31, 2024. FHFA's planned corrective actions meet the intent of our recommendation.

For Recommendation 2, FHFA management partially agreed with this recommendation. On May 9, 2024, FHFA management had fully agreed to this recommendation during the Notification of Findings and Recommendations process. Based on a discussion with an FHFA official on July 1, 2024, it was stated that, prior to receiving the draft report, FHFA management contacted its service provider about updating the service level agreement. The service provider did not agree to update the service level agreement at that time. In lieu of updating the service level agreement, the service provider will provide a monthly background reinvestigation status report.

FHFA management will use the monthly status reports to monitor the status of the background reinvestigation process as a mitigating control. FHFA expects this action to be completed by August 1, 2024. Although FHFA's planned corrective action meets the intent of our recommendation, we encourage FHFA to continue having discussions with the service provider about updating the service level agreement to ensure FHFA receives the necessary information to provide oversight for the background investigation process.

For Recommendation 3, FHFA agreed with this recommendation. FHFA management stated that OFOM will develop and implement the Personnel Security Policy and supporting procedures to monitor and ensure that background reinvestigations for employees and contractors are conducted timely in accordance with FHFA and OPM standards. FHFA expects this action to be completed by June 30, 2025. FHFA's planned corrective actions meet the intent of our recommendation.

For Recommendations 8 and 9, FHFA management agreed with these recommendations. FHFA management stated that, on April 2, 2024, the cloud provider installed an update to automatically disable accounts that have been inactive for more than 365 days. We consider FHFA's corrective actions to meet the intent of our recommendations. Because the remediation occurred after our audit period and is an ongoing process, the remediation of this recommendation will be evaluated in next year's audit.

For Recommendation 10, FHFA management agreed with this recommendation. FHFA management stated that it will update the customer controls for the cloud system and expects this action to be completed by March 30, 2025. FHFA's planned corrective action meets the intent of our recommendation.

For Recommendation 11, FHFA management agreed with this recommendation. FHFA management stated that it will update the overdue SSPPs and Customer Control Plans. FHFA expects this action to be completed by June 30, 2025. FHFA's planned corrective action meets the intent of our recommendation.

For Recommendation 12, FHFA management agreed with this recommendation. FHFA management stated it will work with the system owner to review, update, and test the Capital Models (PolyPaths) ISCP. FHFA expects this action to be completed by March 30, 2025. FHFA's planned corrective action meets the intent of our recommendation.

FHFA-OIG Response

For Recommendations 4 and 7, FHFA-OIG management agreed with these recommendations. FHFA-OIG management stated it has started to implement policies and procedures to oversee FHFA-OIG's background reinvestigation process. The procedures include oversight controls over its service provider and procedural steps for internal suitability adjudicative determinations and suitability actions for covered positions in accordance with OPM's regulation under Title 5 CFR, Part 731.103. FHFA-OIG expects these actions to be completed by October 1, 2024. FHFA-OIG's planned corrective actions meet the intent of our recommendations.

For Recommendations 5 and 6, FHFA-OIG management agreed with these recommendations. FHFA-OIG management stated that FHFA-OIG's service provider has begun to provide monthly background reinvestigation status reports, which FHFA-OIG is using to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely and in accordance with FHFA-OIG and OPM standards. FHFA-OIG's service provider has also committed to include the status reports in its updated service level agreement. FHFA-OIG

expects these actions to be completed by October 1, 2024. FHFA-OIG's planned corrective actions meet the intent of our recommendations.

APPENDIX I – BACKGROUND

Federal Information Security Modernization Act of 2014

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of federal agency information security programs. FISMA requires agency heads[45] to, among other things:

- Be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems; comply with applicable governmental requirements and standards; and ensure information security management processes are integrated with the agency's strategic, operational, and budget planning processes.
- Ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control.
- Delegate to the agency's Chief Information Officer the authority to ensure compliance with FISMA.
- Ensure that the agency has trained personnel sufficient to assist the agency in complying with FISMA requirements and related policies, procedures, standards, and guidelines.
- Ensure that the Chief Information Officer reports annually to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions.
- Ensure that senior agency officials carry out information security responsibilities.
- Ensure that all personnel are held accountable for complying with the agency-wide information security program.

Agencies must also report annually to OMB and to congressional committees on the effectiveness of their information security programs and practices. In addition, FISMA requires agency IGs to assess the effectiveness of their agencies' information security programs and practices.

NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to federal information systems. The standards prescribed include information security standards that provide minimum information security requirements necessary to improve the security of federal information and

[45] 44 U.S. Code (USC) § 3554, *Federal agency responsibilities*.

information systems. FISMA also requires that federal agencies comply with Federal Information Processing Standards issued by NIST. In addition, NIST develops and issues SPs as recommendations and guidance documents.

FISMA Reporting Requirements

OMB and the Department of Homeland Security (DHS) annually provide instructions to federal agencies and IGs for preparing FISMA reports. On December 4, 2023, OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*.[46] This memorandum describes the methodology for conducting FISMA audits and the processes for federal agencies to report to OMB and, where applicable, DHS. The methodology included:

- Selection of 17 supplemental IG FISMA Reporting Metrics that must be evaluated during FY 2024, in addition to the 20 core IG FISMA Reporting Metrics that must be evaluated annually.
- The remainder of standards and controls will be evaluated on a 2-year cycle.
- In previous years, IGs have been directed to use a mode-based scoring approach to assess maturity levels. Beginning in FY 2023, ratings were focused on calculated average scores, wherein the average of the metrics in a particular domain would be used by IGs to determine the effectiveness of individual function areas (Identify, Protect, Detect, Respond, and Recover). IGs were encouraged to focus on the calculated averages of the 20 core IG FISMA Reporting Metrics, as these tie directly to the Administration's priorities and other high-risk areas. In addition, FY 2024 IG FISMA Reporting Metrics indicated that IGs should use the calculated average scores of the supplemental IG FISMA Reporting Metrics, progress in addressing outstanding prior-year recommendations, and other data sources (e.g., FHFA-OIG audits) as data points to support their risk-based determination of overall program and function-level effectiveness. The calculated average scores can be found in the FY 2024 IG FISMA Reporting Metrics, which were provided to the Agency separate from this report.

The FY 2024 IG FISMA Reporting Metrics provided the reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs. As highlighted in **Table 3**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover.

[46] See OMB M-24-04 online here.

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2024 IG FISMA Reporting Metrics

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Identify	Develop an organizational understanding of the business context and the resources that support critical functions to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Risk Management and Supply Chain Risk Management**
Protect	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**
Detect	Implement activities to identify the occurrence of cybersecurity events.	**Information Security Continuous Monitoring**
Respond	Implement processes to take action regarding a detected cybersecurity event.	**Incident Response**
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	**Contingency Planning**

Source: Sikich's analysis of the NIST Cybersecurity Framework and IG FISMA Reporting Metrics.

The foundational levels of the maturity model in the IG FISMA Reporting Metrics focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 4** below explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of Level 4 – *Managed and Measurable*.

Table 4: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess the policies and procedures and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2024 IG FISMA Reporting Metrics

APPENDIX II – OBJECTIVE, SCOPE, AND METHODOLOGY

FHFA-OIG engaged Sikich[47] to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of the Agency's information security programs and practices.

Objective

The objectives of this performance audit were: (1) to evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines, and (2) to respond to the FY *2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2024 IG FISMA Reporting Metrics).[48]

Scope

The scope of this performance audit covered the Agency's information security programs and practices from April 1, 2023, through March 31, 2024. Within this period, we assessed the Agency's information security programs and practices' consistency with FISMA and reporting instructions issued by OMB and DHS for FY 2024. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, supporting the FY 2024 IG FISMA Reporting Metrics for a sample of 4 systems from the 50 systems in FHFA's FISMA inventory of information systems and a sample of 2 systems from the total population of 20 FHFA-OIG FISMA information systems (**Table 5**).

[47] See Footnote 1.

[48] See footnote 4.

Table 5: Description of Systems Selected for Testing

Entity	System	Description
FHFA	AHP Library and Inquiry System	The AHP Library and Inquiry System manages and tracks questions regarding the Affordable Housing Program and the Community Investment Cash Advances Program.
FHFA	General Support System	The FHFA General Support System is considered a Wide Area Network and consists of the backbone, a Metropolitan Area Network, and the Local Area Networks at various sites. The General Support System provides connectivity between the agency's sites, Headquarters, and Datacenters; Internet access; and e-mail and directory services for all Agency divisions and offices.
FHFA	Cloud System	A cloud-based ideation management software that provides a secure software as a service (SaaS) solution for government agencies to make the most of the organizations' collective knowledge.
FHFA	Capital Models (PolyPaths)	Capital Models (PolyPaths) is a web-based pricing and risk management system used by FHFA financial analysts and economists.
FHFA-OIG	Office of Investigations Case Management System (OI-CMS)	OI-CMS is the Office of Investigations' central system for holding case file records and managing investigative resources. The CMS provides management for cases, records, tasks, workflow, and collected items, as well as search and reporting capabilities.
FHFA-OIG	OIGNet General Support System	The FHFA OIGNet General Support System is a general-purpose, multi-user system used throughout FHFA-OIG. Its users are primarily composed of those with desktops and laptops and other ancillary equipment connected to FHFA-OIG network and central servers that support FHFA-OIG. The core network infrastructure consists of network switches, firewalls, and routers that provide boundary protection and network segmentation.

Source: Sikich's analysis of the system descriptions in the system inventories and applicable SSPPs.

For this year's review, IGs were to assess 20 core and 17 supplemental IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area. The maturity levels range from lowest to highest — *Ad-Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized*.

The FY 2023 IG FISMA Reporting Metrics introduced a calculated average scoring model that was continued for the FY 2024 FISMA audits. As part of this approach, core and supplemental IG FISMA Reporting Metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, calculated averages were not automatically rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, OMB strongly encouraged IGs to focus on the results of the core IG FISMA Reporting Metrics, as these tie directly to Administration priorities and other high-risk areas. It was recommended that IGs use the calculated averages of the supplemental IG FISMA Reporting Metrics as a data point to support their risk-based determination of overall program and function-level effectiveness.

We used the FY 2024 IG FISMA Reporting Metrics guidance[49] to form our conclusions for each Cybersecurity Framework domain, function, and the overall agency rating. Specifically, we focused on the calculated average of the core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average of the supplemental IG FISMA Reporting Metrics, progress made in addressing outstanding prior-year recommendations, and

[49] See Footnote 13.

other data sources (e.g., FHFA-OIG audits), to form our risk-based conclusion. For the purposes of this audit, we evaluated each metric for FHFA and FHFA-OIG. Where the metric evaluation results differed, we used a risk-based approach to determine the overall maturity of the metric.

The audit also included an evaluation of whether the Agency took corrective action to address open recommendations from the FY 2020 FISMA audit, FY 2021 FISMA audit, FY 2021 Privacy audit, FY 2023 FISMA audit, and FY 2023 Privacy audit.[50]

Additionally, Sikich took the following audits into consideration to inform the FISMA audit:

- FHFA-OIG 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* (March 8, 2023) (AUD-2023-002).
- FHFA-OIG ongoing internal penetration test audit of FHFA's network and systems (Assignment No. OA-24-005).

We conducted audit fieldwork remotely from October 2023 through June 2024.

We evaluated the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines, and we responded to the FY 2024 IG FISMA Reporting Metrics. Our work did not include assessing the sufficiency of all internal controls over the Agency's information security programs or other matters not specifically outlined in this report. We only assessed security controls directly related to the FY 2024 IG FISMA Reporting Metrics.

Methodology

We conducted this performance audit 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.

To determine if the Agency's information security programs and practices were effective, Sikich conducted interviews with officials and reviewed legal and regulatory requirements stipulated in FISMA. Sikich also reviewed documents supporting the information security program. These documents included, but were not limited to, the Agency's (1) information security policies and procedures, (2) incident response policies and procedures, (3) access control procedures, (4) patch management procedures, (5) change control documentation, and (6) system-generated account listings. Where appropriate, Sikich compared documents, such as IT policies and procedures, to requirements stipulated in relevant OMB memoranda and NIST SPs. In addition, Sikich performed tests of system processes to determine the adequacy and effectiveness of those controls. In addition, Sikich reviewed the status of FISMA and Privacy audit recommendations from FY 2020 through FY 2023. See Appendix III for the status of prior-year recommendations.

In addition, our work in support of the audit was guided by applicable Agency policies and federal standards, including, but not limited to, the following:

[50] See Footnotes 9, 10, 11, and 12.

- *Government Auditing Standards 2018 Revision* (Technical Update April 2021).[51]
- OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* (December 4, 2023).
- OPM's regulation at Title 5 CFR, Part 731.103.
- OPM's regulation at Title 5 CFR, Part 731.106.
- OPM Memorandum, *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Continuous Vetting for Non-Sensitive Public Trust Positions* (March 8, 2024).
- OPM Memorandum, *Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0* (January 15, 2021).
- FY 2024 IG FISMA Reporting Metrics (February 10, 2023).
- NIST SP 800-53, *Revision 5, Security and Privacy Controls for Information Systems and Organizations* (December 10, 2020).
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations* (January 25, 2022).
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (November 11, 2010).
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy*, for the Risk Management Framework controls (December 2018).
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework (April 16, 2018).
- Agency policies and procedures, including but not limited to:
    - *Contingency Planning Standard*, Revision 2.1 (November 30, 2022).
    - *Planning Standard*, Revision 2.1 (November 30, 2022).
    - *Common Control Plan* (May 10, 2023).
    - *FHFA Customer Controls for a Cloud System* (August 1, 2022).
    - *FHFA Personnel Security Standard* (November 30, 2022).
    - *General Support System (OIGNet) System Security Plan (SSP) & Control Implementation Procedures* (May 4, 2023).

[51] While this version was superseded by *Government Auditing Standards 2024 Revision* (February 2024), this version was applicable at the time of this audit.

Sikich selected 4 FHFA systems from the total population of 50 FISMA systems for testing. The four systems were selected based on risk. Specifically, four moderate categorized systems were selected, one being the FHFA General Support System that supports FHFA's applications that reside on the network and the other three being systems that had not been tested in prior years.

Additionally, Sikich selected 2 systems from the total population of 20 FHFA-OIG FISMA systems for testing. The OIGNet was selected based on risk because it is a moderate categorized system that supports FHFA-OIG applications that reside on the network. The Office of Investigations Case Management System was selected because the system had not been tested in prior FISMA audits. Sikich tested the six systems' selected security controls to support its response to the FY 2024 IG FISMA Reporting Metrics.

In testing the adequacy and effectiveness of the security controls, Sikich exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered the relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population.

APPENDIX III – STATUS OF PRIOR RECOMMENDATIONS

The table below summarizes the status of our follow-up related to the status of the open prior recommendations from the FY 2020 FISMA audit (AUD-2021-001), the FY 2021 Privacy audit (AUD-2021-011), the FY 2023 FISMA audit (AUD-2023-004), and the FY 2023 Privacy audit (AUD-2023-006).[52]

Report #/ Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
AUD-2021-001, Finding # 3	We recommend that FHFA management: 3. Implement the planned multi-factor authentication for privileged accounts for internal systems (e.g., infrastructure).	We found that the prior-year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of May 31, 2025.	**Open**
AUD-2021-011, Finding # 2	We recommend that FHFA management: 3. Update the *Privacy Continuous Monitoring Strategy* to ensure that it reflects the FHFA's current privacy control assessment process in accordance with OMB Circular A-130.	We found that the prior-year recommendation has been resolved. The *Privacy Continuous Monitoring Strategy* was updated to reflect the current privacy control assessment process.	**Closed**
AUD-2023-004, Finding #1	We recommend that FHFA's Acting Chief Information Officer: 1. Update FHFA's Supply Chain Risk Management Strategy to include past due OMB M-22-18 requirements including: ○ Obtaining a self-attestation from the software producer before using the software; ○ Obtaining artifacts from software producers that demonstrate conformance to secure software development practices, as needed; ○ Establishing a system to store self-attestation letters from the software producer that are not publicly available in a central location; and ○ Assessing and developing training for reviewing and validating self-attestation letters.	We found that the prior-year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of June 30, 2024.	**Open**

[52] See Footnotes 9, 10, 11, and 12.

Report #/ Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
AUD-2023-004, Finding #1	We recommend that FHFA's Acting Chief Information Officer: 2. If FHFA is unable to meet the requirements in OMB M-22-18 and/or OMB M-23-16 in a timely manner, we recommend that the FHFA Chief Information Officer should consider request for an extension or waiver in accordance with OMB M-22-18 and/or OMB M-23-16. If FHFA requests a waiver, FHFA should consider documenting a risk-based decision and document any compensating controls.	We found that the prior-year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of June 30, 2024.	**Open**
AUD-2023-004, Finding #3	We recommend that FHFA's Acting Chief Information Officer: 3. Remediate past due exploitable vulnerabilities in accordance with CISA's BOD 22-01 and the OTIM Vulnerability Management Process.	We found that the prior-year recommendation has not been resolved and remediation was in progress. FHFA still had past-due exploitable vulnerabilities.	**Open**
AUD-2023-004, Finding #3	We recommend that FHFA's Acting Chief Information Officer: 4. Develop POA&Ms to track the remediation of past due CISA known exploitable vulnerabilities that cannot be remediated in a timely manner (within 14 days) in accordance with CISA's BOD 22-01 and OTIM Vulnerability Management Process. Consider implementing compensating controls (i.e., isolating systems with un-remediated vulnerabilities) to mitigate the risk of the vulnerabilities.	We found that the prior-year recommendation has not been resolved and remediation was in progress. FHFA still had past-due exploitable vulnerabilities.	**Open**
AUD-2023-004, Finding #4	We recommend that FHFA's Acting Chief Information Officer: 5. Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.	We found that the prior-year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of June 30, 2024.	**Open**
AUD-2023-004, Finding #4	We recommend that FHFA's Acting Chief Information Officer: 6. Identify and implement solutions, in coordination with vendors, where a solution	We found that the prior-year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of June 30, 2024.	**Open**

Report #/ Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
	does not exist for systems to natively forward event logs to the security incident and event management tool. If there are no viable solutions, perform a risk assessment and cost benefit analysis. Based on the risk assessment, document any risk-based decisions, including compensating controls, for systems not in compliance with OMB M-21-31.		
AUD-2023-004, Finding #5	We recommend that FHFA-OIG's Chief Information Officer: 7. Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.	We found that the prior-year recommendation has been resolved. FHFA-OIG completed implementation across all EL maturity levels to ensure events are logged and tracked in accordance with OMB M-21-31.	**Closed**
AUD-2023-004, Finding #5	We recommend that FHFA-OIG's Chief Information Officer: 8. Identify and implement solutions, in coordination with vendors and engineering team, to encrypt logs in transit between the source system and SIEM tool. If there are no viable solutions, perform a risk assessment and cost benefit analysis. Based on the risk assessment, document any risk-based decisions, including compensating controls, for systems not in compliance with OMB M-21-31.	We found that the prior-year recommendation has been resolved. FHFA-OIG documented risk-based decisions that consider compensating controls for OMB M-21-31 compliance, as applicable.	**Closed**
AUD-2023-004, Finding #6	We recommend that FHFA's Acting Chief Information Officer: 9. Review and update the *Cyber Incident Reporting Procedures*, and the *FHFA Common Control Plan* to ensure they include FHFA's three-year review cycle outlined in the Incident Response Standard.	We found that the prior-year recommendation has been resolved. The *Cyber Incident Reporting Procedures, Incident Reporting Procedures,* and *Common Control Plan* were updated to incorporate the 3-year review cycle.	**Closed**
AUD-2023-004, Finding #7	We recommend that FHFA's Acting Chief Information Officer: 10. Update the *Disaster Recovery Procedures for FHFA Production Systems* to include Job Performance Plan (JPP) and its servers, and	We found that the prior-year recommendation has not been resolved and remediation remains in progress. The *Disaster Recovery Procedures for FHFA Production Systems* was not fully updated to address JPP structured query language servers.	**Open**

Report #/ Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
	ensure they are included in the annual contingency testing.		
AUD-2023-006, Finding #1	We recommend that FHFA-OIG's Chief Counsel: 1. Update the *FHFA-OIG Privacy Program Plan* to include procedures to verify personnel's completion of annual role-based privacy training. Procedures should include periodic progress checks and follow-up with personnel to ensure timely training completion.	We found that the prior-year recommendation has been resolved. FHFA-OIG updated the *FHFA-OIG Privacy Program Plan* to include procedures to verify personnel's completion of annual role-based privacy training.	**Closed**
AUD-2023-006, Finding #2	We recommend that FHFA's Senior Agency Official for Privacy (SAOP): 2. Revise the FHFA Privacy Program Plan to document the frequency of review for existing privacy impact assessments (PIAs) in accordance with OMB Circular No. A-130.	We found that the prior-year recommendation has been resolved. The *FHFA Privacy Program Plan* has been revised to define the frequency of PIA review to be every 3 years.	**Closed**
AUD-2023-006, Finding #2	We recommend that FHFA's SAOP, in coordination with the System Owner and Chief Information Security Officer (CISO): 3. Ensure that all required approval signatures are captured within the PIA and maintain a record of review for each PIA, as required by the FHFA Privacy Impact Assessment Guide.	We found that the prior-year recommendation has been resolved. The *Privacy Security Questionnaire and Privacy Impact Assessment Guide* (February 2024) was updated to include procedures detailing that the final PIA should be reviewed by the System/Collection Owner, the Senior Agency Information Security Officer (SAISO), and the SAOP. Further, we noted that PIAs for our in-scope systems had all required signatures, as applicable.	**Closed**
AUD-2023-006, Finding #2	We recommend that FHFA's SAOP: 4. Update the PIAs for the Emergency Notification System, the National Mortgage Database (NMDB), and the cloud system to ensure PIAs accurately describe all security and privacy controls of the system and are approved by the required officials.	We found that the prior-year recommendation has been resolved. The Emergency Notification System, NMDB, and the cloud system PIAs were updated and approved.	**Closed**
AUD-2023-006, Finding #3	We recommend that FHFA's SAOP, in coordination with the originating office and the Office of General Counsel: 5. Obtain and review proposed rules, and determine if a PIA is required, in accordance with FHFA Policy No. 801, Official Documents Policy.	We found that the prior-year recommendation has been resolved. FHFA included the Privacy Office in the electronic clearance process for all rulemakings before they are published in the Federal Register. From June through December 2023, the three proposed rules and one final rule underwent Privacy Office Review.	**Closed**

APPENDIX IV – MANAGEMENTS' COMMENTS

FHFA's Management Comments

Federal Housing Finance Agency

MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audits

THROUGH: Katrina D. Jones, Chief Operating Officer /s/

FROM: Luis Campudoni, Chief Information Officer /s/

SUBJECT: Draft Audit Report: Audit of the Federal Housing Finance Agency's Information Security Programs and Practices, Fiscal Year 2024

DATE: June 28, 2024

Thank you for the opportunity to respond to the above-referenced draft audit report (Report) by the Office of Inspector General (OIG), which contains 12 recommendations. This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the eight recommendations specific to FHFA in the Report. As FHFA's new Chief Information Officer, I am pleased to respond to this report and to address the recommendations OIG has provided. The Report also makes four recommendations (Recommendations 4, 5, 6 and 7) specific to the FHFA OIG, who will respond in a separate memorandum.

Recommendation 1: Develop and implement policies and procedures to oversee FHFA's background reinvestigation process, including oversight controls over FHFA's service provider.

FHFA's Recommendation 1 Response: FHFA agrees with Recommendation 1. FHFA's Office of Facilities Management (OFOM) will develop and implement policies and procedures to oversee the Agency's background reinvestigation process, including oversight controls over FHFA's service provider by December 31, 2024.

Recommendation 2: Update the service level agreement between FHFA and the service provider to include requirements for the service provider to provide background reinvestigation status reports on a regular basis.

FHFA's Recommendation 2 Response: FHFA partially agrees with Recommendation 2. IBC will provide monthly background reinvestigation status reports starting on August 1, 2024. FHFA will use the monthly IBC status report to monitor the status of the background reinvestigation process.

Recommendation 3: *Implement a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance with FHFA and OPM standards.*

FHFA's Recommendation 3 Response: OFOM will perform the following steps by June 30, 2025:

1. Develop and implement the Personnel Security Policy; and
2. Develop and implement procedures to support the Personnel Security Policy which monitor and ensure that background reinvestigations for employees and contractors are conducted timely in accordance with FHFA and OPM standards.

Recommendation 8: Disable accounts of non-privileged users who have been inactive for over 365 days, as required by the FHFA customer controls for the cloud system.

Recommendation 9: Work with the cloud system's vendor to implement software updates that automatically disable user accounts after 365 days of inactivity, as required by the FHFA customer controls for the cloud system.

FHFA's Recommendations 8 and 9 Response: FHFA agrees with Recommendations 8 and 9. On April 2, 2024, the cloud provider installed an update to automatically disable accounts that have been inactive for over 365 days. No further action is required to address these recommendations.

Recommendation 10: Update the customer controls for the cloud system to include a procedure for regular reviews of non-privileged users' access.

FHFA's Recommendation 10 Response: FHFA agrees with Recommendation 10 and will update the cloud system customer controls by March 30, 2025.

Recommendation 11: Complete the review and update of overdue SSPPs and Customer Control Plans in accordance with the existing, related POA&Ms.

FHFA's Recommendation 11 Response: FHFA agrees with Recommendation 11 and will update the overdue System Security and Privacy Plans (SSPPs) and Customer Control Plans by June 30, 2025.

Recommendation 12: Complete the review, update, and testing of the Capital Models (PolyPaths) ISCP in accordance with the existing, related POA&M.

FHFA's Recommendation 12 Response: FHFA agrees with Recommendation 12. OTIM will work with the system owner to review, update, and test the ISCP by March 30, 2025.

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

cc: Joshua Stallings
Edom Aweke
Jason Donaldson
Tom Leach
Tasha Cooper
Ralph Mosios
John Major

SIKICH®

FHFA-OIG's Management Comments

OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

July 1, 2024

TO: Sikich CPA LLP

THRU: Adam Silverman, Deputy Inspector General for Administration /s/

FROM: Michael Smith, Chief Information Officer /s/

SUBJECT: Draft Audit Report: Performance Audit of the Federal Housing Finance Agency's Information Security Programs and Practices for 2024

Thank you for the opportunity to respond to Sikich's audit of the Federal Housing Finance Agency's (FHFA) and the FHFA Office of Inspector General's (FHFA-OIG) information security programs and practices for fiscal year 2024. We trust that the results of this independent audit will provide assurance to our stakeholders that FHFA-OIG's Information Security Program and practices are operating effectively in compliance with FISMA legislation, OMB guidance, and NIST Special Publications. These independent audit results confirm that our Information Technology infrastructure, policies, procedures and practices are suitably designed and implemented to provide reasonable assurance of adequate security.

This memorandum provides FHFA-OIG's management response to the four recommendations applicable to our office.

Recommendation 4: *Develop and implement policies and procedures to oversee FHFA-OIG's background reinvestigation process, including oversight controls over FHFA-OIG's service provider.*

Recommendation 5: *Update the service level agreement between FHFA-OIG and the service provider to include requirements for the service provider to provide background reinvestigation status reports on a regular basis.*

Recommendation 6: *Implement a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance with FHFA-OIG and OPM standards.*

Recommendation 7: *Establish and implement a process to make suitability adjudicative determinations and take suitability actions for covered positions in accordance with OPM's regulation under Title 5 CFR Part 731.103.*

Management Response to Recommendations 4, 5, 6, and 7: FHFA-OIG concurs with the recommendations and has already initiated the following actions in response. To address these recommendations, FHFA-OIG met with both the U.S. Office of Personal Management (OPM)

and FHFA-OIG's service provider in April, May, and June 2024. As a result of those meetings, FHFA-OIG's service provider has begun to provide monthly background reinvestigation status reports, which FHFA-OIG is using to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely and in accordance with FHFA-OIG and OPM standards. FHFA-OIG's service provider has also committed to include the status reports in its updated service level agreement no later than October 1, 2024. (Recommendations 5 and 6)

In addition, to support the transition of the personnel security adjudicatory function from the service provider to FHFA-OIG, six FHFA-OIG employees attended the OPM Fundamentals of Suitability for Suitability and Fitness Adjudicators courses offered in May and June 2024; the six are now certified to make suitability and fitness for duty determinations for FHFA-OIG. FHFA-OIG has started to implement policies and procedures to oversee FHFA-OIG's background reinvestigation process, including oversight controls over its service provider and procedural steps for internal suitability adjudicative determinations and suitability actions for covered positions in accordance with OPM's regulation under Title 5 CFR Part 731.103. This will be completed no later than October 1, 2024. (Recommendations 4 and 7)

If you have any questions, please feel free to contact Michael S. Smith, Chief Information Officer, FHFA-OIG, 202-730-0401, michael.smith@fhfaoig.gov.

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