Federal Housing Finance Agency
Office of Inspector General

Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025

Audit Report • AUD-2025-004 • July 30, 2025

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

July 30, 2025

TO: 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 2025* (AUD-2025-004)

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 to determine the effectiveness of such program and practices.

Pursuant to FISMA, we contracted with Sikich CPA LLC (herein referred to as "Sikich"), a certified independent public accounting firm, to conduct the fiscal year (FY) 2025 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. Sikich conducted its 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 2025 Inspector General 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 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 maturity Level 3 – *Consistently Implemented*. Sikich identified 4 new weaknesses in 3 of the 6 Cybersecurity Functions and within 3 of the 10 IG FISMA Metric domains. To address these weaknesses, Sikich made six 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 16, 2025, 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.

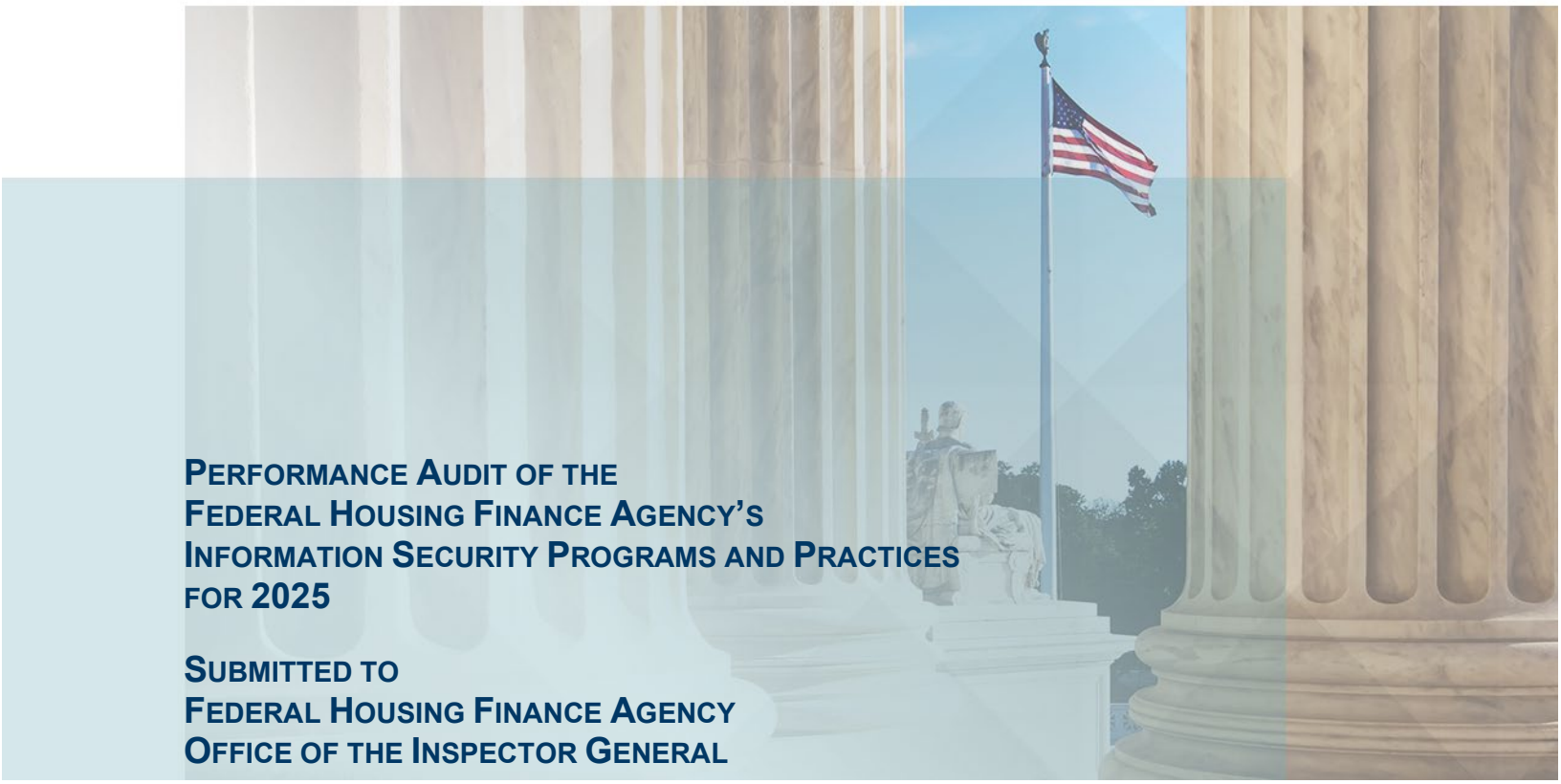
As discussed in Sikich's report, the Agency's management agreed with the recommendations and outlined its plans to address them.

Attachment

ATTACHMENT

Audit of the Federal Housing Finance Agency's
Information Security Programs and Practices
Fiscal Year 2025

SIKICH®



PERFORMANCE AUDIT OF THE FEDERAL HOUSING FINANCE AGENCY'S INFORMATION SECURITY PROGRAMS AND PRACTICES FOR 2025

SUBMITTED TO
FEDERAL HOUSING FINANCE AGENCY
OFFICE OF THE INSPECTOR GENERAL

PERFORMANCE AUDIT REPORT

JULY 16, 2025

SIKICH®

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

SIKICH.COM

July 16, 2025

John Allen
Acting Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024

Dear Acting Inspector General Allen:

Sikich CPA LLC (Sikich) conducted a performance audit of the Federal Housing Finance Agency's (FHFA) and the 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, 2025, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). In addition, FISMA requires agencies to develop, implement, and document an agency-wide information security program. FISMA also requires Inspectors General (IG) to conduct an annual independent evaluation of their agencies' information security programs and practices. We performed this audit under contract with the FHFA-OIG.

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) 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (FY 2025 IG FISMA Reporting Metrics). The audit covered the period from April 1, 2024, through March 31, 2025. We conducted audit fieldwork remotely and onsite at FHFA headquarters in Washington DC, from October 2024 through May 2025.

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. We describe our objectives, scope, and methodology in **Appendix II: Objective, Scope, and Methodology.**

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.

Sikich CPA LLC

Alexandria, VA

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) 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) 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (FY 2025 IG FISMA Reporting Metrics).[1]

OMB and the Department of Homeland Security (DHS) provide instructions to Federal agencies and IGs for preparing annual FISMA reports. On January 15, 2025, OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*[2] which provides reporting guidance for FY 2025 in accordance with FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders collaborated to develop the FY 2025 IG FISMA Reporting Metrics.

The FY 2025 IG FISMA Reporting Metrics require us to assess the maturity of six function areas in the Agency's information security programs and practices. For this year's review, IGs were required to assess 20 core[3] and 5 supplemental[4] IG FISMA Reporting Metrics across six function areas—Govern[5], Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agencies' information security program and the maturity level of each

[1] See the FY 2025 IG FISMA Reporting Metrics online here.

[2] See OMB Memorandum M-25-04 online here.

[3] Core metrics are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine the effectiveness of a security program. The core metrics can be found in the FY 2025 IG FISMA Reporting Metrics online here.

[4] Supplemental metrics are not considered a core metric but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. The supplemental metrics can be found in the FY 2025 IG FISMA Reporting Metrics online here.

[5] The *NIST Cybersecurity Framework (CSF) 2.0* was published in February 2024, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an entity's enterprise risk management strategy. As such, the FY 2025 IG FISMA Reporting Metrics added a new IG FISMA function (Govern) that includes a new domain (Cybersecurity Governance) to align with CSF 2.0.

function area.[6] 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* or higher. See **Appendix I** for additional information on the FY 2025 IG FISMA Reporting Metrics and FISMA reporting requirements.

The scope of this performance audit included the Agency's information security programs and practices covering the period from April 1, 2024, through March 31, 2025. We conducted audit fieldwork remotely and onsite at FHFA headquarters in Washington DC, from October 2024 through May 2025.

For this audit, Sikich reviewed selected controls from NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the FY 2025 IG FISMA Reporting Metrics, for a sample of Agency information systems[7] in the Agency's FISMA inventories of information systems.

We concluded that the Agency complied with FISMA and related information security policies and procedures, standards, and guidelines. However, we determined 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. In this audit, we identified 4 weaknesses in 3 of 6 Cybersecurity Framework (CSF) functions, and within 3 of the 10 IG FISMA Metric domains. As a result, we made 6 new recommendations to assist the Agency in strengthening its information security programs and practices.

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 2024

At the beginning of our performance audit, there were 20 open recommendations from prior FISMA audits (1 open recommendation from the FY 2020 FISMA audit,[8] 7 open recommendations from the FY 2023 FISMA audit,[9] and 12 from the FY 2024 FISMA audit).[10]

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

[7] 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.

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

[9] 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).

During this audit, the Agency took corrective actions to address 12 of these recommendations, and we consider them closed. Corrective actions are in progress on the other 8 open recommendations. Refer to **Appendix III** for a detailed description and status of each recommendation.

Current Status

We concluded that the Agency complied with FISMA and related information security policies and procedures, standards, and guidelines. However, we determined that the Agency's information security programs were not effective. Specifically, we noted that one CSF function achieved a maturity of Level 4 – *Managed and Measurable*, two CSF functions achieved a maturity of Level 3 – *Consistently Implemented*, and three CSF functions achieved a maturity of Level 2 – *Defined*. Since five of the six CSF functions did not reach Level 4 – *Managed and Measurable*, the Agency's information security programs did not meet the criteria for effectiveness. As a result, the Agency's overall maturity was rated as Level 3 – *Consistently Implemented* (Not Effective). **Table 1** shows a summary of the overall maturity levels for each function and domain in the FY 2025 IG FISMA Reporting Metrics.

Table 1: Maturity Levels for FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Functions[11]	Maturity Level by Function	Domain	Maturity Level by Domain
Govern	Level 2: Defined (Not Effective)	Cybersecurity Governance	Level 2: Defined (Not Effective)
		Cybersecurity Supply Chain Risk Management	Level 2: Defined (Not Effective)
Identify	Level 3: Consistently Implemented (Not Effective)	Risk and Asset Management	Level 3: Consistently Implemented (Not Effective)
Protect	Level 2: Defined (Not Effective)	Configuration Management	Level 2: Defined (Not Effective)
		Identity and Access Management	Level 2: Defined (Not Effective)
		Data Protection and Privacy	Level 2: Defined (Not Effective)
		Security Training	Level 3: Consistently Implemented (Not Effective)
Detect	Level 3: Consistently Implemented (Not Effective)	Information Security Continuous Monitoring	Level 3: Consistently Implemented (Not 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 2025 IG FISMA Reporting Metrics.

[10] FHFA-OIG Audit Report AUD-2024-006, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2024* (July 30, 2024).

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

In accordance with the FY 2025 IG FISMA Reporting Metrics guidance,[12] 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 or risk indicators (e.g., FHFA-OIG audits) to come to this risk-based conclusion. As a result, we rated the Agency's overall maturity level as Level 3 – *Consistently Implemented* (Not Effective).

In this audit, we identified four weaknesses in the Cybersecurity Governance, Identity and Access Management, and Contingency Planning domains of the FY 2025 IG FISMA Reporting Metrics (see Findings 1 through 4 in **Table 2**). As such, we made six recommendations to assist the Agency in strengthening its information security programs and practices. These weaknesses, in combination with prior year open FISMA audit recommendations and weaknesses noted in FHFA-OIG audits,[13] significantly impacted the Agency's overall information security programs and practices. Specifically, the Agency needs to improve controls over Cybersecurity Governance, Cybersecurity Supply Chain Risk Management, Risk and Asset Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. **Table 2** below maps weaknesses to FY 2025 IG FISMA Reporting Metrics functions and domains and includes weaknesses related to the Agency's 8 open prior-year recommendations (refer to **Appendix III**) and weaknesses from FHFA-OIG audits that impact the FY 2025 IG FISMA Reporting Metrics. The weaknesses from the 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. These key weaknesses need to be addressed in a comprehensive manner to achieve an effective rating of Level 4 – *Managed and Measurable.*

Table 2: Weaknesses Noted in FISMA Audit Mapped to the CSF Functions and Domains in the FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Functions	IG FISMA Reporting Metrics Domain	Weaknesses Noted
Govern	Cybersecurity Governance	FHFA did not implement the *NIST CSF 2.0* (**Finding 1**).
	Cybersecurity Supply Chain Risk Management	FHFA-OIG's audit report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2023* (July 26, 2023) (AUD-2023-004), had an open prior-year recommendation related to obtaining

[12] The FY 2025 IG FISMA Reporting Metrics provided the agency IG the discretion to determine the rating for each of the CSF domains and functions and the overall agency rating based on their evaluations. 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.

[13] The following FHFA-OIG audits that impacted the FY 2025 IG FISMA Reporting Metrics were taken into consideration: *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), *FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement* (September 25, 2024) (AUD-2024-010), and FHFA-OIG's ongoing external penetration test of FHFA's network and systems (Assignment No. OA-25-008).

Cybersecurity Framework Functions	IG FISMA Reporting Metrics Domain	Weaknesses Noted
		software attestations and/or waivers from vendors.
Identify	Risk and Asset Management	FHFA-OIG's audit report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2024* (July 30, 2024) (AUD-2024-006), had an open prior-year recommendation related to reviewing System Security and Privacy Plans. FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), revealed shortcomings related to software management controls.
Protect	Configuration Management	FHFA-OIG's audit report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2023* (July 26, 2023) (AUD-2023-004), had an open prior-year recommendation related to remediating vulnerabilities in a timely manner. FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), revealed shortcomings related to configuration management controls. Based on consultation with FHFA-OIG regarding its ongoing external penetration test of FHFA's network and systems, noted risk areas for this domain.
	Identity and Access Management	FHFA-OIG's audit report, *Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2020* (October 20, 2020) (AUD-2021-001), had an open prior-year recommendation related to implementing planned multi-factor authentication for privileged accounts for internal systems. FHFA did not approve privileged accounts prior to provisioning access (**Finding 2**). FHFA did not disable inactive network accounts (**Finding 3**). FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007), revealed shortcomings related to access controls.
	Data Protection and Privacy	FHFA-OIG's audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats*

Cybersecurity Framework Functions	IG FISMA Reporting Metrics Domain	Weaknesses Noted
		(August 12, 2024) (AUD-2024-007), revealed shortcomings related to data protection and privacy controls.
	Security Training	FHFA not testing Disaster Recovery Plans (DRPs) on an annual basis, revealed weaknesses related to System Owner turnover (**Finding 4**).
Detect	Information Security Continuous Monitoring	FHFA-OIG's audit report, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2024* (July 30, 2024) (AUD-2024-006), had an open prior-year recommendation related to reviewing System Security and Privacy Plans.
Respond	Incident Response	Based on consultation with FHFA-OIG regarding its ongoing external penetration test of FHFA's network and systems, noted risk areas for this domain.
Recover	Contingency Planning	FHFA did not test Disaster Recovery Plans (DRPs) on an annual basis (**Finding 4**). FHFA-OIG's audit report, *FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement,* (September 25, 2024) (AUD-2024-010), revealed shortcomings related to contingency planning.

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. FHFA Did Not Implement NIST's CSF 2.0

CSF Function: *Govern*
FY 2025 IG FISMA Reporting Metrics Domain: *Cybersecurity Governance*

FHFA did not implement the *NIST CSF 2.0* (February 26, 2024)[14] through its policies and procedures. Specifically, FHFA did not document its guidance for performing CSF 2.0 activities, such as developing and maintaining both current and target cybersecurity profile(s).[15]

According to an FHFA Office of the Chief Information Officer (OCIO) official, OCIO experienced significant leadership turnover and staff departures during the transition to new FHFA leadership. The same official also noted that FHFA has developed a number of policies and procedures related to CSF 2.0 implementation, but that additional efforts remain due to aforementioned impacts. However, OCIO management could not provide evidence of documented guidance for CSF 2.0 activities.

The Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* (Green Book) (September 2014), states the following regarding management's responsibility for implementing control activities:

> *Principle 12.01: Management should implement control activities through policies.*
>
> *Principle 12.02: Management documents in policies the internal control responsibilities of the organization.*

Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), required that:

> *Each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework)[16] developed by NIST, or any successor document, to manage the agency's cybersecurity risk.*

The absence of documented guidance for utilizing the CSF 2.0 increases the risk that cybersecurity risks may not be appropriately planned for or addressed. Further, this may increase the risk to the following, but not limited to, breaches, system interruptions, and vulnerabilities being exploited.

We recommend the FHFA Chief Information Officer:

---

[14] See *The NIST CSF 2.0* online here.

[15] *The NIST CSF 2.0* (February 26, 2024), provides guidance to assist with managing cybersecurity risks. Section 3.1 offers guidance on the use of cybersecurity profiles to understand, tailor, assess, prioritize and communicate cybersecurity objectives. A CSF Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes. The CSF Core is a taxonomy of high-level cybersecurity outcomes that can help organizations manage their cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome.

[16] Before version 2.0, the Cybersecurity Framework was called the "Framework for Improving Critical Infrastructure Cybersecurity." This title is not used for CSF 2.0.

- **Recommendation 1:** Establish and implement guidance for performing CSF 2.0 activities through policies and procedures.

2. FHFA Did Not Approve Privileged Accounts Prior To Provisioning Access

CSF Function: *Protect*
FY 2025 IG FISMA Reporting Metrics Domain: *Identity and Access Management*

FHFA did not fully complete and approve Privileged Account Request eWorkflows[17] for 3 of the total 11 FHFA General Support System (GSS) privileged user accounts created between April 1, 2024, to January 21, 2025. Specifically, the required process workflow steps[18]—Approver Review, Manager Review, and Implementation—were not completed before access was provisioned for these three accounts.

An FHFA OCIO official stated that the three incomplete eWorkflows were likely the result of an unintentional system owner oversight.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (December 10, 2020), security control Access Control (AC-2) (Account Management), requires that organizations authorize access to the system based on a valid access authorization.

FHFA Account Management Guidelines (November 30, 2022), Table 2, requires that privileged accounts be requested and approved via the Privileged Account Request eWorkflow.

FHFA Common Control Plan (November 21, 2024), security control AC-2 (1), (Account Management | Automated System Management), requires that Privileged Accounts are requested via eWorkflows and once approved, OCIO engineers create the applicable account or assign the approved permission.

The absence of fully completed and approved Privileged Account Request eWorkflows may increase the risk that privileged users could be given access to data and systems that exceeds their roles and responsibilities. This could result in unintentional disclosure of sensitive or confidential information, privileged access misuse, and reduced accountability for system changes.

We recommend the FHFA Chief Information Officer:

- **Recommendation 2:** Ensure that Privileged Account Request eWorkflows are fully completed and approved for all privileged FHFA GSS user accounts prior to granting access.

[17] Privileged accounts are requested through eWorkflows through FHFA's Identity and Access Management tool and once approved, engineers create the applicable account or assign the approved permission. The approval record is the Privileged Account Request eWorkflow.

[18] The Privileged Account Request eWorkflow consisted of the following process workflow steps: Initiate Request, Information System Security Officer Review, X-Account Creation, Approver Review, Manager Review, Implementation, and Completion.

3. FHFA Did Not Disable Inactive Network Accounts

CSF Function: *Protect*
FY 2025 IG FISMA Reporting Metrics Domain: *Identity and Access Management*

Based on review of FHFA's Active Directory (AD) User Listing as of January 21, 2025, we found that 9 of 1,603 enabled user accounts (approximately .6 percent) were not disabled after 35 days of inactivity.

An FHFA OCIO official stated that the affected accounts were test accounts housed in an AD Organizational Unit (OU)[19] labeled "Domain User Accounts/Test Users". These test accounts were not subject to the automated process that disables accounts after 35 days of inactivity.

Another FHFA OCIO official stated that FHFA OCIO determined that the testing associated with the test accounts was completed; however, the official could not provide an exact timeframe for when the testing was completed. The same FHFA OCIO official stated that since the test accounts were no longer needed for testing purposes, the test accounts were deleted from AD after Sikich informed FHFA management of this issue.

NIST SP 800-53, Revision 5, security 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.

FHFA's *System Security and Privacy Plan (SSPP) for the General Support System (GSS)* (December 4, 2024), security control AC-2(2) (Account Management | Automated Temporary and Emergency Account Management), states that the Active Administrator[20] automatically disables all AD Accounts within the Domain Admins and Domain User Account OU's after 35 days of inactivity.

By not deactivating user accounts, an insider could gain unauthorized access to sensitive information and privileges. This access could be further used to extract sensitive information from FHFA systems without being detected.

We recommend the FHFA Chief Information Officer:

- **Recommendation 3:** Ensure all applicable OUs are included in the automated process that disables inactive accounts after 35 days.
- **Recommendation 4:** Disable inactive AD accounts after a period of 35 days of inactivity.

[19] OUs are container objects in Active Directory that allow you to organize and manage your network resources, including users, computers, and other objects.

[20] Active Administrator is a Microsoft AD administration tool.

4. FHFA Did Not Test Disaster Recovery Plans On An Annual Basis

CSF Function: *Recover*
FY 2025 IG FISMA Reporting Metrics Domain: *Contingency Planning*

FHFA did not test the *Disaster Recovery Procedures for FHFA Production Systems (DRP)*[21] annually for three of four[22] FHFA systems selected for testing. Specifically, we noted that FHFA did not test any aspect of the following systems' DRP procedures annually (from April 1, 2024, through March 31, 2025).[23]

- FHFA GSS[24]
- Office of General Counsel (OGC) Matter Management Tracking System[25]
- FHFA Status Tracking and Reporting (STAR) System[26]

An FHFA OCIO official stated that the DR exercises were not scheduled and planned for the three systems; and management does not have an estimated timeframe on when future exercises would be performed. In addition, the same official stated that system owners who are responsible for carrying out the DR test have left FHFA. Therefore, system-related Information System Contingency Plan (ISCP) testing has not occurred, and there is no estimation for future exercises at this time. FHFA is in various stages of assigning new system owners, but they will require training on their roles and responsibilities.

Further, the same official stated that a Plan of Action and Milestones (POA&M) was not established for not testing the DRP for the three systems.

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.

---

[21] FHFA's DRP constitutes the Information System Contingency Plan, which applies to several systems, including the GSS, Office of General Counsel (OGC) Matter Management Tracking System, and FHFA Status Tracking and Reporting (STAR) system. The DRP contains the steps to recover critical IT services in the event of a disruption. The DRP assigns the responsibility and authority to the Disaster Recovery Coordinator, in conjunction with the organization's administrative leadership, to take whatever steps necessary to identify, respond, contain, and eradicate the impact of an IT disaster.

[22] The fourth system in scope for testing was a cloud-based system that FHFA utilizes to track the processing of Freedom of Information Act (FOIA) and Privacy Act requests. As a cloud-based system, the cloud provider is responsible for conducting contingency plan tests.

[23] The last Disaster Recovery (DR) exercise was split into two parts and performed between November 3 - 5, 2023 and March 22, 2024. The first part of the DR test encompassed rolling over primary computing services (Active Directory Services and Citrix Remote access). The second part of the DR test encompassed restoring the SQL server infrastructure for three specific applications.

[24] The FHFA GSS is considered a Wide Area Network and consists of the backbone, a Metropolitan Area Network, and the Local Area Networks at various sites. The GSS provides connectivity between the FHFA's sites, Headquarters, and data centers; Internet access; and e-mail and directory services for all FHFA divisions and offices.

[25] The OGC Matters Management Tracking System is utilized to track OGC projects and activities.

[26] The STAR system supports the electronic creation and maintenance of issues existing between the FHFA, as Conservator, and the Enterprises (Fannie Mae and Freddie Mac).

FHFA's *Contingency Planning Standard,* Revision 2.2 (September 30, 2024), requires that FHFA 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.

By not annually testing the DRP, FHFA may not be able to determine the effectiveness of its DRP and the organizational readiness to execute the plan in the event of a disaster. As such, FHFA's OCIO may not be fully aware of the potential risks during the exercise and may not recover the system successfully or timely during a disruption.

We recommend the FHFA Chief Information Officer:

- **Recommendation 5:** Create a POA&M to establish when the annual DRP exercise will be conducted and when the new system owners will be assigned and trained on their roles and responsibilities related to FHFA GSS, OGC Matter Management Tracking System, and the STAR system.
- **Recommendation 6:** Schedule and conduct an annual DRP exercise for the FHFA GSS, OGC Matter Management Tracking System, and the STAR system, and ensure new system owners are trained to execute them.

IV. Evaluation of Managements Comments

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

FHFA Response

For Recommendation 1, FHFA management agreed with this recommendation. FHFA management stated that they will develop a CSF Implementation Plan for utilizing CSF 2.0. FHFA expects this action to be completed by October 31, 2025. FHFA's planned corrective action meets the intent of our recommendation.

For Recommendation 2, FHFA management agreed with this recommendation. FHFA management stated that the Account Request eWorkflows for the three FHFA GSS privileged user accounts were completed. We consider FHFA's corrective action to meet the intent of our recommendation and would encourage FHFA management to ensure all Account Request eWorkflows are fully completed in the future. 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 3, FHFA management agreed with this recommendation. FHFA management stated that applicable OUs have been included in the automated process that disables inactive accounts after 35 days. We consider FHFA's corrective action to meet the intent of our recommendation. 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 4, FHFA management agreed with this recommendation. FHFA management stated that it has disabled the identified test AD accounts and subsequently deleted them. We consider FHFA's corrective actions to meet the intent of our recommendation. 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 Recommendations 5 and 6, FHFA management agreed with these recommendations. FHFA management stated that DRP exercises for the GSS, OGC Matter Management Tracking System and the STAR system had recently been completed. FHFA management stated that since the DRP exercises have been completed, POA&Ms to track completion were no longer needed. We consider FHFA's corrective actions to meet the intent of our recommendation. Because the remediation occurred after our audit period, the remediation of these recommendations will be evaluated in next year's audit.

FHFA-OIG Response

FHFA-OIG did not have any new findings and recommendations identified in this report. FHFA-OIG management thanked Sikich for the opportunity to respond to the report.

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[27] 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. These include standards prescribed minimum security requirements and best practices to protect federal systems. In addition, NIST develops and issues Federal Information Processing Standards (FIPS), and also publishes SPs as recommendations and guidance documents.

[27] 44 U.S. Code (USC) § 3554, *Federal agency responsibilities*.

FISMA Reporting Requirements

OMB and DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On January 15, 2025, OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* which provides reporting guidance for FY 2025 in accordance with FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. As a result, OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders collaborate to develop these metrics.

One of the goals of the annual FISMA evaluations is to assess agencies' progress toward achieving objectives that strengthen Federal cybersecurity. The FY 2025 IG FISMA Reporting Metrics were updated to reflect recent developments:

- NIST published the CSF 2.0 in February 2024, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's enterprise risk management strategy. As such, a new IG FISMA function *(Govern)* was added that includes a new domain (*Cybersecurity Governance)* to align with CSF 2.0.
- To align with the CSF 2.0, the Supply Chain Risk Management domain moved from the *Identify* function to the *Govern* function and remains to better reflect the agency oversight of supply chain risk.
- A new domain, Risk and Asset Management, was introduced in the Identify function to group metrics on system inventory, and hardware, software, and data management.
- Five supplemental metrics are in scope for the FY 2025 IG FISMA evaluation, including two new supplemental metrics that are focused on system level risk management practices critical to achieving Zero Trust Architecture objectives.
- The core metric on information system level risk management was revised to focus on the maturity of agencies' implementation of the NIST Risk Management Framework.

As highlighted in **Table 3**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and practices and align with the six function areas in the NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover.

Table 3: Alignment of the CSF Functions to the Domains in the FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	**Cybersecurity Governance and Cybersecurity Supply Chain Risk Management**
Identify	The organization's current cybersecurity risks are understood.	**Risk and Asset Management**
Protect	Safeguards to manage the organization's cybersecurity risks are used.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	**Information Security Continuous Monitoring**

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Respond	Actions regarding a detected cybersecurity incident are taken.	**Incident Response**
Recover	Assets and operations affected by a cybersecurity incident are restored.	**Contingency Planning**

Source: Sikich's analysis of the NIST CSF 2.0 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 at least 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 2025 IG FISMA Reporting Metrics

APPENDIX II: OBJECTIVE, SCOPE, AND METHODOLOGY

FHFA-OIG engaged Sikich 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 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (FY 2025 IG FISMA Reporting Metrics).

Scope

The scope of this performance audit covered the Agency's information security programs and practices from April 1, 2024, through March 31, 2025. 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 2025. The scope of the audit also included assessing selected controls from NIST SP 800-53, Revision 5, supporting the FY 2025 IG FISMA Reporting Metrics, for a sample of 4 systems from the 51 systems in FHFA's FISMA inventory of information systems and a sample of 2 systems from the total population of 22 FHFA-OIG FISMA information systems (**Table 5**).

Table 5: Description of Systems Selected for Testing

Entity	System	Description
FHFA	Cloud System	A cloud-based, software as a service (SaaS) solution that tracks the processing of Freedom of Information Act (FOIA) and Privacy Act (PA) requests.
FHFA	GSS	The FHFA GSS 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.
FHFA	OGC MTS	System to track OGC projects and activities.
FHFA	STAR	The Division of Conservatorship STAR system supports the electronic creation and maintenance of issues existing between the FHFA, as Conservator, and the Enterprises.
FHFA-OIG	Cyber Investigations Unit Digital Analysis Laboratory (CIULAB)	The CIU-Lab supports the FHFA-OIG Office of Investigations. The CIU-Lab is comprised of multiple standalone, off-network systems to support investigators and case prosecutors in the collection, storage, and review of digital evidence.
FHFA-OIG	OIGNet GSS	The FHFA OIGNet GSS 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 5 supplemental FY 2025 IG FISMA Reporting Metrics across six function areas — Govern, 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 2023-2024 IG FISMA Reporting Metrics* introduced a calculated average scoring model that was continued for the FY 2025 FISMA audits. As part of this approach, core and supplemental IG FISMA Reporting Metrics were averaged independently to determine a domain's maturity level 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 2025 IG FISMA Reporting Metrics guidance[28] to form our conclusions for each CSF function, domain, 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 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 2023 FISMA audit, and FY 2024 FISMA audit.[29]

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

- FHFA-OIG audit report, *FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats* (August 12, 2024) (AUD-2024-007).
- FHFA-OIG audit report, *FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement* (September 25, 2024) (AUD-2024-010).

In addition, we consulted with FHFA-OIG regarding its ongoing external penetration test of FHFA's network and systems that may impact the FY 2025 FISMA audit.

We conducted audit fieldwork remotely and onsite at FHFA headquarters in Washington DC, from October 2024 through May 2025.

[28] The FY 2025 IG FISMA Reporting Metrics provided the agency IG the discretion to determine the rating for each of the CSF domains and functions and the overall agency rating based on their evaluations. 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.

[29] See Footnotes 8, 9, and 10.

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 Agency officials and reviewed legal and regulatory requirements stipulated in FISMA. Sikich also reviewed documents supporting the information security programs. 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 information technology 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 audit recommendations from FY 2020 through 2024. 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 guidelines and standards, including, but not limited to, the following:

- *Government Auditing Standards 2018 Revision* (Technical Update April 2021).[30]
- GAO's *Standards for Internal Control in the Federal Government* (Green Book) (September 2014).
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* (January 15, 2025).
- *FY 2025 IG FISMA Reporting Metrics v2.0* (April 3, 2025).
- 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).
- The *NIST Cybersecurity Framework (CSF) 2.0* (February 26, 2024).
- Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017).
- Agency policies and procedures, including but not limited to:
    - *FHFA Account Management Guidelines* (November 30, 2022).
    - FHFA's *Common Control Plan* (November 21, 2024).
    - FHFA's *Contingency Planning Standard,* Revision 2.2 (September 30, 2024).

[30] While GAO issued *Government Auditing Standards 2024 Revision* in February 2024, the 2018 revision was still applicable as FHFA-OIG had not implemented the 2024 revision at the time of this audit. Full implementation of the 2024 revision is for audits beginning on or after December 15, 2025.

- FHFA's *System Security and Privacy Plan (SSPP) for the General Support System (GSS)* (December 4, 2024).

Sikich judgmentally selected 4 FHFA information systems from the total population of 51 systems in FHFA's FISMA inventory of information systems for testing. The four systems were judgmentally selected based on risk. Specifically, four moderate categorized systems were selected, one being the FHFA GSS 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 judgmentally selected 2 information systems from the total population of 22 FHFA-OIG FISMA information 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 CIU-LAB 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 2025 IG FISMA Reporting Metrics.

We assessed internal controls that we deemed to be significant to the audit objectives. Specifically, we assessed 3 of the 17 principles associated with the 5 components of internal control defined in the GAO's *Standards for Internal Controls in the Federal Government* (September 2014) (the Green Book). The table below summarizes the principles we assessed:

Table 6: GAO Green Book Assessed Principles

Control Activities
Principle 10: Management should design control activities to achieve objectives and respond to risks.
Principle 11: Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
Principle 12: Management should implement control activities through policies.

We assessed the design, implementation, and/or operating effectiveness of these internal controls and identified deficiencies that we believe could affect the Agency's information security programs and practices. The internal control deficiencies we found are discussed in the Audit Findings section of this report. However, because our review was limited to aspects of these internal control components and underlying principles related to the Agency's information security programs and practices, it may have not disclosed all internal control deficiencies that may have existed at the time of this audit.

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 2023 FISMA audit (AUD-2023-004), and the FY 2024 FISMA audit (AUD-2024-006).[31]

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 completed. FHFA is in the process of creating a plan to address the requirement through procedural and technical means. At the time of this report, management did not have an estimated completion date for remediation.	**Open**
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 been completed. The FHFA's *Supply Change Risk Management Strategy* was updated to include OMB-M-22-18 requirements.	**Closed**

[31] See Footnotes 8, 9, and 10.

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 completed. Management did not request extensions and/or waivers from OMB for past due software attestations in accordance with OMB M-22-18 and/or OMB M-23-16. FHFA management stated that they have contacted OMB and have been advised to submit a risk acceptance to OMB for review. At the time of this report, management did not provide an estimated completion date for remediation.	**Open**
AUD-2023-004, Finding #3	We recommend that FHFA's Acting Chief Information Officer: 3. Remediate past due exploitable vulnerabilities in accordance with Cybersecurity and Infrastructure Security Agency (CISA)'s Binding Operational Directive (BOD) 22-01 and the *OTIM Vulnerability Management Process*.	We found that the prior-year recommendation has not been completed. FHFA still had past due vulnerabilities. At the time of this report, management did not provide an estimated completion date for remediation.	**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 been completed. FHFA is creating POA&Ms on a quarterly basis to track the remediation of outstanding, aged vulnerabilities.	**Closed**
AUD-2023-004, Finding #4	We recommend that FHFA's Acting Chief Information Officer: 5. Implement requirements across all Event Logging (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 completed. FHFA completed implementation across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.	**Closed**
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 does not exist for systems to	We found that the prior-year recommendation has been completed. FHFA implemented EL maturity Tiers to ensure events are logged and tracked in accordance with OMB M-21-31.	**Closed**

Report #/ Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
	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 #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 ensure they are included in the annual contingency testing.	We found that the prior-year recommendation has been completed. The *Disaster Recovery Procedures for FHFA Production Systems* was updated to include JPP and its servers in the annual contingency testing.	**Closed**
AUD-2024-006, Finding #1	We recommend that the FHFA Chief Information Officer, in coordination with the Associate Director for Agency Operations: 1. Develop and implement policies and procedures to oversee FHFA's background reinvestigation process, including oversight controls over FHFA's service provider.	We found that the prior-year recommendation has not been completed and remediation was in progress. Management provided an estimated completion date of May 30, 2025. On May 22,2025, FHFA provided a closure package for this prior year recommendation. The package consisted of the *Office of Chief Operating Officer, Standard Operating Procedure (SOP), Personnel Security Policy* (May 13, 2025). Since the corrective actions occurred after the audit period, the implementation of the policy will be evaluated during the next audit period.	**Open**
AUD-2024-006, Finding #1	We recommend that the FHFA Chief Information Officer, in coordination with the Associate Director for Agency Operations: 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.	We found that the prior-year recommendation has been completed. While FHFA and the service provider could not agree upon an update to the service level agreement; the service provider did agree to provide a report of background investigation status on-demand that may be utilized by management for oversight purposes.	**Closed**
AUD-2024-006, Finding #1	We recommend that the FHFA Chief Information Officer, in coordination with the Associate Director for Agency Operations: 3. Implement a process to monitor and ensure that background reinvestigations for relevant employees and contractors are conducted timely in accordance	We found that the prior-year recommendation has not been completed and remediation was in progress. Management provided an estimated completion date of June 30, 2025.	**Open**

Report #/ Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
	with FHFA and Office of Personnel Management (OPM) standards.		
AUD-2024-006, Finding #2	We recommend that FHFA-OIG's Chief Information Officer, in coordination with the Director of Human Resources: 4. Develop and implement policies and procedures to oversee FHFA-OIG's background reinvestigation process, including oversight controls over FHFA-OIG's service provider.	We found that the prior-year recommendation has been completed. FHFA-OIG developed and implemented policies and procedures to oversee FHFA-OIG's background reinvestigation process, including oversight controls over FHFA-OIG's service provider.	**Closed**
AUD-2024-006, Finding #2	We recommend that FHFA-OIG's Chief Information Officer, in coordination with the Director of Human Resources: 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.	We found that the prior-year recommendation has been completed. The service level agreement between FHFA-OIG and the service provider was updated to include requirements for the service provider to provide background reinvestigation status reports.	**Closed**
AUD-2024-006, Finding #2	We recommend that FHFA-OIG's Chief Information Officer, in coordination with the Director of Human Resources: 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.	We found that the FHFA-OIG is in the process of implementing its remediation plan, but that plan is not yet completed. Management provided an estimated completion date of December 31, 2025.	**Open**
AUD-2024-006, Finding #2	We recommend that FHFA-OIG's Chief Information Officer, in coordination with the Director of Human Resources: 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.	We found that the FHFA-OIG is in the process of implementing its remediation plan, but that plan is not yet completed. Management provided an estimated completion date of December 31, 2025.	**Open**
AUD-2024-006, Finding #3	We recommend that FHFA's Chief Information Officer: 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.	We found that the prior-year recommendation has been completed. FHFA management is no longer utilizing the cloud system and has retired the system.	**Closed**
AUD-2024-006, Finding #3	We recommend that FHFA's Chief Information Officer: 9. Work with the cloud system's vendor to implement software updates that automatically disable user	We found that the prior-year recommendation has been completed. FHFA management is no longer utilizing the cloud system and has retired the system.	**Closed**

Report #/ Finding #	Recommendation	Agency Actions Taken	Auditor's Position on Status
	accounts after 365 days of inactivity, as required by the FHFA customer controls for the cloud system.		
AUD-2024-006, Finding #3	We recommend that FHFA's Chief Information Officer: 10. Update the customer controls for the cloud system to include a procedure for regular reviews of non-privileged users' access.	We found that the prior-year recommendation has been completed. FHFA management is no longer utilizing the cloud system and has retired the system.	**Closed**
AUD-2024-006, Finding #4	We recommend that FHFA's Chief Information Officer: 11. Complete the review and update of overdue SSPPs and Customer Control Plans in accordance with the existing related POA&Ms.	We found that the prior-year recommendation has not been completed and remediation was in progress. Management provided an estimated completion date of June 30, 2025.	**Open**
AUD-2024-006, Finding #5	We recommend that FHFA's Chief Information Officer: 12. Complete the review, update, and testing of the Capital Models (PolyPaths) ISCP in accordance with the existing related POA&M.	We found that the prior-year recommendation has been completed. The Capital Models (PolyPaths) ISCP was reviewed, updated and tested.	**Closed**

APPENDIX IV: MANAGEMENTS COMMENTS

FHFA's Management Comments

Federal Housing Finance Agency

MEMORADUM

TO: James Hodge, Deputy Inspector General for Audits

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 2025*

DATE: June 30, 2025

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) draft report. The objective of audit was to (1) to evaluate the effectiveness of the Agency's information security programs and practices, including compliance with Federal Information Security Modernization Act of 2014 (FISMA) and related information security policies, procedures, standards, and guidelines, and (2) to respond to the fiscal year (FY) 2025 Inspector General FISMA Reporting Metrics. The audit evaluated the Agency's information security programs, practices, and remediation efforts from April 1, 2024, through March 31, 2025.

We are pleased the audit determined that the Agency complied with FISMA and related information security policies and procedures, standards, and guidelines. However, the audit rated the Agency's overall program maturity at a Level 3, *Consistently Implemented,* and identified recommendations to strengthen information security controls. Management's responses and planned actions are outlined below.

Recommendation 1: *Establish and implement guidance for performing CSF 2.0 activities through policies and procedures.*

Management Response: FHFA agrees with the recommendation and will develop a Cybersecurity Framework Implementation Plan for utilizing CSF 2.0 by October 31, 2025.

Recommendation 2: *Ensure that Privileged Account Request eWorkflows are fully completed and approved for all privileged FHFA GSS user accounts prior to granting access.*

Management Response: FHFA agrees with the recommendation. The Office of the Chief Information Officer (OCIO) has completed the Account Request eWorkflows for the three FHFA General Support System (GSS) privileged user accounts. OCIO will provide OIG with documentation from the completed account request eWorkflows.

Recommendation 3: *Ensure all applicable OUs are included in the automated process that disables inactive accounts after 35 days.*

Management Response: FHFA agrees with the recommendation. OCIO has confirmed that applicable organizational units (OUs) have been included in the automated process that disables inactive accounts after 35 days. OCIO will provide OIG with documentation on this effort.

Recommendation 4: *Disable inactive AD accounts after a period of 35 days of inactivity.*

Management Response: FHFA agrees with the recommendation. OCIO has addressed this recommendation by disabling the identified test Active Directory (AD) accounts and subsequently deleting them. OCIO has provided OIG with documentation on this effort.

Recommendation 5: *Create a POA&M to establish when the annual DRP exercise will be conducted and when the new system owners will be assigned and trained on their roles and responsibilities related to FHFA GSS, OGC Matter Management Tracking System, and the STAR system.*

Management Response: FHFA agrees with the recommendation. OCIO recently completed disaster recovery plan (DRP) exercises for the GSS, OGC Matter Management Tracking System, and STAR system. Since the exercises have been completed, Plans of Action & Milestones (POAMs) to track completion are not needed. OCIO will provide the OIG with documentation from the completed exercises.

Recommendation 6: *Schedule and conduct an annual DRP exercise for the FHFA GSS, OGC Matter Management Tracking System, and the STAR system, and ensure new system owners are trained to execute them.*

Management Response: FHFA agrees with the recommendation. As noted above, OCIO completed DRP exercises for the GSS, OGC Matter Management Tracking System, and STAR system. OCIO will provide the OIG with documentation from the completed exercises.

cc: Marcus Williams
Jeffery Harris
Derrick Bumbrey
Warren Hammonds
John Major

FHFA-OIG's Management Comments

OFFICE OF INSPECTOR GENERAL

Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

June 23, 2025

TO: Sikich

THRU: Brian W. Baker, Deputy Inspector General for Administration /s/

FROM: Michael S. Smith, Chief Information Officer /s/

SUBJECT: Draft Audit Report: Performance Audit of the Federal Housing Finance Agency's Information Security Programs and Practices for 2025

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 2025. 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.

We appreciate Sikich's professionalism in conducting this year's audit. If you have any questions, please feel free to contact me at 202-730-0401 or 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