Federal Housing Finance Agency
Office of Inspector General

Audit of the Federal Housing Finance Agency's Information Security Program and Practices Fiscal Year 2022

Audit Report • AUD-2022-009 • July 28, 2022

OFFICE OF INSPECTOR GENERAL

Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

July 28, 2022

TO: Jason Donaldson, Acting 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 Program and Practices Fiscal Year 2022* (AUD-2022-009)

We are pleased to transmit the subject report.

The Federal Information Security Modernization Act of 2014 (FISMA) requires the Federal Housing Finance Agency (FHFA) to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, FISMA mandates that federal agencies undergo an annual independent evaluation of its information security program and practices.

Pursuant to FISMA, we contracted with CliftonLarsonAllen LLP (CLA) to conduct the fiscal year (FY) 2022 independent evaluation of FHFA's and FHFA Office of Inspector General's (hereafter collectively referred to as FHFA) information security program as a performance audit under generally accepted government auditing standards. The objectives of the audit were to (1) evaluate the effectiveness of FHFA's information security program and practices, including FHFA's compliance with FISMA-related information security policies, procedures, standards, and guidelines; and (2) respond to the Office of Management and Budget (OMB) Office of the Federal Chief Information Officer *FY22 Core IG Metrics Implementation Analysis and Guidelines* (FY 2022 IG FISMA Metrics). For this audit, CLA reviewed selected controls mapped to the FY 2022 IG FISMA Metrics for a sample of information systems in FHFA's FISMA system inventory.

Based on the selected controls and the sampled information systems reviewed, CLA concluded that FHFA implemented an effective information security program and complied with FISMA and related information security policies and procedures, standards, and guidelines by achieving an overall *Managed and Measurable* maturity level. Although FHFA implemented an effective information security program, its implementation of a subset of selected controls was not fully effective. Specifically, CLA reported two findings: (1) Weaknesses with Mobile Device Patch Management and (2) Weaknesses in Legal Cost Control (LCC) Simple Invoice Management System (SIMS) Audit Logging.

In connection with the contract, we reviewed CLA'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 FHFA's implementation of its information security program and compliance with FISMA and related information security policies, procedures, standards, and guidelines. CLA is responsible for the attached auditor's report dated July 14, 2022, and the conclusions expressed therein. Our review found no instances where CLA did not comply, in all material respects, with generally accepted government auditing standards.

As discussed in the auditor's report, FHFA 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 Program and Practices
Fiscal Year 2022

Audit of the Federal Housing Finance Agency's Information Security Program and Practices

Fiscal Year 2022

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
CLAconnect.com

July 14, 2022

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

Dear Inspector General Tomney:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the results of our audit of Federal Housing Finance Agency (FHFA or Agency) and FHFA Office of Inspector General's (FHFA-OIG's) (hereafter collectively referred to as FHFA) information security program and practices for fiscal year 2022 in accordance with the Federal Information Security Modernization Act of 2014. We performed this audit under contract with the FHFA-OIG.

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

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

Very truly yours,

S. M Mirzakhani

Sarah Mirzakhani, CISA
Principal

Inspector General
Federal Housing Finance Agency

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Federal Housing Finance Agency (FHFA or Agency) and FHFA Office of Inspector General's (FHFA-OIG) (hereafter collectively referred to as FHFA) information security program and practices for fiscal year 2022 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA or the Act). FISMA requires agencies to develop, implement, and document an agency-wide information security program. The Act also requires Inspectors General to conduct an annual independent evaluation of their agencies' information security program and practices.

The objectives of this performance audit were to (1) evaluate the effectiveness of FHFA's information security program and practices, including FHFA's compliance with FISMA and related information security policies, procedures, standards, and guidelines; and (2) respond to the Office of Management and Budget (OMB) Office of the Federal Chief Information Officer *Fiscal Year (FY) 2022 Core Inspector General (IG) Metrics Implementation Analysis and Guidelines* (FY 2022 Core 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, Inspectors General were required to assess 20 Core IG Metrics in 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.[1] 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 FHFA's information security programs and practices consistent with FISMA and reporting instructions issued by OMB. The scope also included assessing selected security controls outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for a sample of systems in FHFA's FISMA inventory of information systems.

Audit fieldwork covered FHFA's headquarters located in Washington DC, from February 2022 to June 2022. The audit covered the period from July 1, 2021 through June 30, 2022.

We concluded that FHFA implemented an effective information security program and complied with FISMA and related information security policies and procedures, standards, and guidelines by achieving an overall *Managed and Measurable* maturity level. Although FHFA implemented an effective information security program, its implementation of a subset of selected controls was not fully effective. Specifically, we noted weaknesses in two of the nine domains in the FY 2022

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

Core IG FISMA Reporting Metrics. As a result, we make three recommendations to assist FHFA in strengthening its information security program.

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

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
July 14, 2022

Table of Contents

EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA or the Act) 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 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 (FIPS) to establish agency baseline security requirements.

The Federal Housing Finance Agency Office of Inspector General (FHFA-OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of FHFA and FHFA-OIG's (hereafter collectively referred to as FHFA) information security program and practices.

The objectives of this performance audit were to (1) evaluate the effectiveness of the FHFA's information security program and practices, including FHFA's compliance with FISMA and related information security policies, procedures, standards, and guidelines; and (2) respond to the Office of Management and Budget (OMB) Office of the Federal Chief Information Officer *Fiscal Year (FY) 2022 Core Inspector General (IG) Metrics Implementation Analysis and Guidelines* (FY 2022 Core IG FISMA Reporting Metrics).

The FY 2022 Core IG FISMA Reporting Metrics requires us to assess the maturity of five functional areas in FHFA's information security program and practices. For this year's review, Inspectors General were required to assess 20 Core Metrics in 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.[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*. See Appendix I for additional information on the FY 2022 Core IG FISMA Reporting Metrics and FISMA reporting requirements.

For this audit, CLA reviewed selected controls mapped to the FY 2022 Core IG FISMA Reporting Metrics for a sample of information systems[3] in FHFA's FISMA inventory of information systems.[4]

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.

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

[3] 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.

[4] FHFA's FISMA inventory of information systems details a list of FHFA's FISMA reportable systems.

Audit Results

Progress Since FY 2021

At the beginning of FY 2022, there were 14 open recommendations from prior FISMA and Privacy audits (2 open recommendations from the FY 2019 Privacy audit,[5] 1 open recommendation from the FY 2019 FISMA audit,[6] 3 open recommendations from the FY 2020 FISMA audit,[7] 5 open recommendations from the FY 2021 Privacy audit,[8] and 3 open recommendations from the FY 2021 FISMA audit[9]). During the course of the audit, we found that FHFA took corrective actions to address 6 recommendations and we consider those recommendations closed. Corrective action is in progress on the other 8 open recommendations. Refer to Appendix III for a detailed description of the status of each recommendation.

Current Status

We concluded that FHFA implemented an effective information security program and practices and complied with FISMA and related information security policies and procedures, standards, and guidelines by achieving an overall Level 4 – *Managed and Measurable* maturity level. **Table 1** below shows a summary of the overall maturity levels for each domain in the FY 2022 Core IG FISMA Reporting Metrics.

Table 1: Maturity Levels for FY 2022 Core IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Domain	Maturity
Identify ***Overall Identify Function Maturity Level: Consistently Implemented***	**Risk Management**	Level 3: Consistently Implemented
	Supply Chain Risk Management	Level 3: Consistently Implemented
Protect ***Overall Protect Function Maturity Level: Level 4: Managed and Measurable***	**Configuration Management**	Level 3: Consistently Implemented
	Identity and Access Management	Level 4: Managed and Measurable
	Data Protection and Privacy	Level 3: Consistently Implemented
	Security Training	Level 5: Optimized

[5] FHFA-OIG Audit Report AUD-2019-009, *Audit of the Federal Housing Finance Agency's 2019 Privacy Program*, issued August 28, 2019.
[6] FHFA-OIG Audit Report AUD-2020-001, *Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2019*, issued October 25, 2019.
[7] FHFA-OIG Audit Report AUD-2021-001, *Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2020*, issued October 20, 2020.
[8] FHFA-OIG Audit Report AUD-2021-011, *Audit of the Federal Housing Finance Agency's 2021 Privacy Program*, issued August 11, 2021.
[9] FHFA-OIG Audit Report AUD-2022-001, *Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2021*, issued October 15, 2021.

Cybersecurity Framework Security Functions	Domain	Maturity
Detect	**Information Security Continuous Monitoring**	Level 4: Managed and Measurable
Respond	**Incident Response**	Level 3: Consistently Implemented
Recover	**Contingency Planning**	Level 4: Managed and Measurable
Overall		**Level 4: Managed and Measurable - Effective**

Although we concluded that FHFA implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted weaknesses in two of the nine domains of the FY 2022 Core IG FISMA Reporting Metrics (see **Table 2**) and have made three recommendations to assist FHFA in strengthening its information security program. In response to a draft of this report, FHFA agreed with all three recommendations made in this report and outlined its plans to address each recommendation.

Table 2: Weaknesses Noted in FY 2022 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2022 Core IG FISMA Reporting Metrics

Cybersecurity Framework Security Function	FY 2022 Core IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	No weaknesses noted.
	Supply Chain Risk Management	No weaknesses noted.
Protect	**Configuration Management**	Weaknesses with Mobile Device Patch Management (**Finding 1**)
	Identity and Access Management	Weaknesses in Legal Cost Control (LCC) Simple Invoice Management System (SIMS) Audit Logging (**Finding 2**)
	Data Protection and Privacy	No weaknesses noted.
	Security Training	No weaknesses noted.
Detect	**Information Security Continuous Monitoring**	No weaknesses noted.
Respond	**Incident Response**	No weaknesses noted.
Recover	**Contingency Planning**	No weaknesses noted.

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 FHFA's management comments.

AUDIT FINDINGS

1. Weaknesses with Mobile Device Patch Management

Cybersecurity Framework Security Function: *Protect*
FY 2022 Core IG FISMA Reporting Metrics Domain: *Configuration Management*

FHFA did not ensure all mobile devices had the minimally accepted operating system (OS) version installed. As of May 12, 2022, 50 out of 847 mobile devices were not running FHFA's minimally accepted OS version (i.e., within one version of the last major OS release 15.4.1) as required by FHFA's *Mobile Device Patch Management Procedure.*

A Supervisory Information Technology Specialist stated that FHFA completed their annual mobile device review during November 2021. Office of Technology and Information Management (OTIM) Security distributed an email on November 10, 2021, to remind users to update their mobile device's OS version. The email stated that the deadline for updating mobile devices was November 15, 2021, and if the devices OS version was not updated, then the devices would be disabled on November 17, 2021. According to the same Supervisory Information Technology Specialist, FHFA's Chief Information Officer made a risk-based decision to temporarily suspend the policy to disable non-compliant devices, since FHFA was working in a maximum telework status due to the COVID-19 pandemic. We could not validate FHFA's risk-based decision assertion because it was not documented.

FHFA's *Mobile Device Patch Management Procedure*, dated April 8, 2021, Section 2.5, requires that on an annual basis, OTIM Security review all FHFA managed mobile devices and contact users whose devices are not within one version of the last major OS release. OTIM Security will notify users of devices running an older OS version to update their device by a target date determined by FHFA's Chief Information Security Officer (CISO) and disable devices that have not been updated by the target date.

NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, Security Control System and Information Integrity (SI) – 2 Flaw Remediation, requires organizations to identify, report, and correct system flaws; and to install security-relevant software and firmware updates.

Mobile OS updates patch publicly known security vulnerabilities and often introduce new features, as well as fix any known issues in the OS and core applications. Failure to update mobile devices' OS versions to a minimally accepted OS version increases the risk that the mobile devices containing FHFA data can be compromised.

We recommend that FHFA's Chief Information Officer:

> ***Recommendation 1:*** *Update the mobile devices running below the minimally acceptable OS version or disable the devices in accordance with FHFA's Mobile Device Patch Management Procedure.*
>
> ***Recommendation 2:*** *Document any risk-based decision, including compensating controls, to temporarily deviate from FHFA's Mobile Device Patch Management Procedures, as necessary.*

2. Weaknesses in LCC SIMS Audit Logging

Cybersecurity Framework Security Function: *Protect*
FY 2022 Core IG FISMA Reporting Metrics Domain: *Identity and Access Management*

LCC provides independent verification and validation support to FHFA for reviewing legal invoices and supporting documentation. LCC utilizes its SIMS, a web-based application, to upload and analyze FHFA legal invoices and supporting documentation. The security controls over SIMS are a shared responsibility between LCC and FHFA. LCC is responsible for maintaining technical[10] and operational[11] security controls for SIMS. FHFA is responsible for ensuring SIMS is operating in accordance with FHFA security policies and standard. FHFA documents the controls it is responsible for in the FHFA’s *Customer Controls For LCC SIMS.*

FHFA did not review and analyze audit log records[12] for the LCC SIMS on a defined basis for unusual or suspicious activity.

The LCC SIMS System Owner stated the *Customer Controls for LCC SIMS* did not establish a process for generating audit log records for review and analysis on a defined basis. However, audit log records for LCC SIMS are maintained in its database and an audit log records report can be generated for review.

NIST SP 800-53, Revision 5, Security Control Audit and Accountability, (AU) - 6, Audit Record Review, Analysis, and Reporting, requires that the organization review and analyze system audit records on a defined basis for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.

Failure to establish a process for generating audit log records for review and analysis for LCC SIMS increases the risk that FHFA may not be aware of unusual or suspicious activity. This may, in turn increase the risk that FHFA may inadvertently miss the potential scope and/or veracity of suspicious events and/or attacks.

We recommend that FHFA’s Chief Information Officer:

> ***Recommendation 3:*** *Establish and implement a process to generate and review audit log records for LCC SIMS on a defined basis within the Customer Controls for LCC SIMS.*

[10] The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

[11] The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

[12] Audit record content that may be necessary to support the auditing function may include event descriptions, time stamps, source and destination addresses, user or process identifiers, and success or fail indications. Event outcomes include indicators of event success or failure and event-specific results.

EVALUATION OF MANAGEMENT COMMENTS

In response to a draft of this report, FHFA management agreed with all three recommendations made in this report and outlined its plans to address each recommendation. FHFA’s comments are included in Appendix IV.

For recommendation 1, FHFA management agrees with this recommendation. FHFA management indicated that as of June 30, 2022, all mobile devices comply with the FHFA’s *Mobile Device Patch Management Procedure* and that no further action will be taken on this recommendation*.* To the extent that FHFA updated the mobile devices running below the minimally acceptable OS versions or disabled the devices in accordance with FHFA’s *Mobile Device Patch Management Procedure,* we consider the intent of the recommendation met. Since mobile device patch management is an on-going process, the remediation of this recommendation will be evaluated in next year’s audit.

For recommendation 2, FHFA management agrees with this recommendation. FHFA stated that they will update the *Mobile Device Patch Management Procedure* to clarify that exceptions will be documented and approved by the CISO, including compensating controls, if needed. This action will be completed by September 30, 2022. We consider FHFA’s planned corrective action to meet the intent of this recommendation.

For recommendation 3, FHFA management agrees with this recommendation. FHFA plans to retire the LCC SIMS application by December 31, 2022. If the LCC SIMS application is not retired, then FHFA will work with the vendor to implement a process to receive and review audit logs monthly by March 15, 2023. We consider FHFA’s planned corrective action to meet the intent of this recommendation.

BACKGROUND

Overview

Established by the Housing and Economic Recovery Act of 2008, Public Law 110-289, FHFA is an independent Federal agency with a Director appointed by the President and confirmed by the United States Senate. The Agency's mission is to provide effective supervision, regulation, and housing mission oversight of Fannie Mae; Freddie Mac; Common Securitization Solutions, LLC; the 11 Federal Home Loan Banks (FHLBanks), and the FHLBanks' fiscal agent, the Office of Finance. FHFA is a non-appropriated, non-apportioned agency that draws its financial resources from assessments on Fannie Mae, Freddie Mac, and the FHLBanks.

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[13] to, among other things:

1. 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; complying with applicable governmental requirements and standards; and ensuring information security management processes are integrated with the agency's strategic, operational, and budget planning processes.
2. Ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control.
3. Delegate to the agency Chief Information Officer the authority to ensure compliance with FISMA.
4. Ensure that the agency has trained personnel sufficient to assist the agency in complying with FISMA requirements and related policies, procedures, standards, and guidelines.
5. Ensure that the Chief Information Officer reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.
6. Ensure that senior agency officials carry out information security responsibilities.
7. Ensure that all personnel are held accountable for complying with the agency-wide information security program.

[13] 44 USC § 3554, Federal agency responsibilities.

Agencies must also report annually to OMB and to congressional committees on the effectiveness of their information security program. In addition, FISMA requires agency Inspectors General to assess the effectiveness of their agency's information security program 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 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 Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On December 6, 2021, OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes key changes to the methodology for conducting FISMA audits; and the processes for Federal agencies to report to OMB, and where applicable, DHS. Key changes to the methodology included:

- Selection of a core group of 20 metrics and highly valuable controls that must be evaluated annually.
- The remainder of standards and controls will be evaluated on a two – year cycle.
- OMB shifted the due date of the IG FISMA Reporting Metrics from October to July to better align with the release of the President's Budget.
- Use of this reporting timeline began in FY 2022 starting with the Core Metrics.

The FY 2022 Core IG FISMA Reporting Metrics provided the reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.

For this year's review, Inspectors General were to assess 20 Core Metrics in 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 Core 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, as highlighted in **Table 3**.

Federal Housing Finance Agency
FY 2022 Audit of FHFA's Information Security Program and Practices

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2022 Core IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Domains in the FY 2022 Core IG FISMA Reporting Metrics
Identify	Risk Management, Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The foundational levels of the maturity model in the Core 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. The table 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 strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy 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 strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objectives of this performance audit were to (1) evaluate the effectiveness of the FHFA's information security program and practices, including FHFA's compliance with FISMA and related information security policies, procedures, standards, and guidelines; and (2) respond to the FY 2022 Core IG FISMA Reporting Metrics.

Scope

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, Inspectors General were to assess 20 Core Metrics in 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 scope of this performance audit was to assess FHFA's information security program consistent with FISMA, and reporting instructions issued by OMB and DHS. The scope also included assessing selected security controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for a sample of four systems from the 44 systems in FHFA's FISMA inventory of information systems and one system from the total population of 17 FHFA-OIG FISMA information systems **(Table 5)**.

Table 5: Description of Systems Selected for Testing

Organization	System Name	Description
FHFA	Competency Assessment System	The Competency Assessment System is a web-based application used by FHFA employees and supervisors to assess and examine employee's proficiency for the competencies within the Competency Model established for the employee's respective position.
FHFA	General Support System (GSS)	FHFA GSS is considered a Wide Area Network (WAN) and consists of the backbone, a Metropolitan Area Network, and the Local Area Networks (LAN) at various sites. The GSS provides connectivity between the agency's sites, Headquarters, and Datacenters; Internet access; and e-mail and directory services for all agency divisions and offices.

Organization	System Name	Description
FHFA	GovDelivery	The GovDelivery Communications Cloud is a Software as a Service (SaaS) Community Cloud offered by GovDelivery to Federal, state and local government organizations.
FHFA	LCC SIMS	LCC provides independent verification and validation support to FHFA for reviewing legal invoices and supporting documentation. LCC utilizes its SIMS, a web-based application, to upload and analyze FHFA legal invoices and supporting documentation.
FHFA-OIG	OIGNet	The FHFA OIGNet GSS is a general purpose, multi-user system used throughout FHFA-OIG. It is composed of users primarily with desktops and laptops and other ancillary equipment connected via FHFA-OIG network to central servers that support FHFA-OIG. The core network infrastructure consists of network switches, firewalls, and routers that provide boundary protection and network segmentation.

The audit also included an evaluation of whether FHFA took corrective action to address open recommendations from the FY 2019 FISMA audit, FY 2019 Privacy audit, FY 2020 FISMA audit, FY 2021 FISMA audit, and FY 2021 Privacy audit.[14]

Additionally, CLA leveraged the following related FHFA-OIG audit reports in evaluating FHFA's information security program and practices:

- FHFA-OIG Audit Report, AUD-2022-003, *FHFA Did Not Follow All of its Contingency Planning Requirements for the National Mortgage Database (NMDB) or its Correspondence Tracking System (CTS)*, issued December 13, 2021.
- FHFA-OIG Audit Report, AUD-2021-009, *FHFA Did Not Record, Track, or Report All Security Incidents to US-CERT; 38% of Sampled FHFA Users Did Not Report a Suspicious Phone Call Made to Test User Awareness of its Rules of Behavior*, issued June 25, 2021.

Audit fieldwork covered FHFA headquarters located in Washington DC, from February 2022 to June 2022. The audit covered the period from July 1, 2021 through June 30, 2022.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in this report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. The information included in this report was obtained from FHFA on or before July 14, 2022. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to July 14, 2022.

[14] Ibid. footnotes 5,6, 7, 8, and 9.

Methodology

To determine if FHFA implemented an effective information security program, CLA conducted interviews with FHFA officials and reviewed legal and regulatory requirements stipulated in FISMA. Also, CLA reviewed documents supporting the information security program. These documents included, but were not limited to, FHFA'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, CLA compared documents, such as FHFA's IT policies and procedures, to requirements stipulated in NIST special publications. In addition, CLA performed tests of system processes to determine the adequacy and effectiveness of those controls. In addition, CLA reviewed the status of FISMA and Privacy audit recommendations from FY 2019 through FY 2021. See Appendix III for the status of prior year recommendations.

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

- OMB Memorandum M-22-05 *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.
- FY 2022 Core IG FISMA Reporting Metrics.
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* for specification of security controls.
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations,* for the assessment of security control effectiveness.
- 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.
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).
- FHFA policies and procedures, including but not limited to: *FHFA's Mobile Device Patch Management Procedure, and Customer Controls for LCC SIMS.*

CLA selected four FHFA systems from the total population of 44 FISMA reportable systems for testing. The four systems were selected based on risk. Specifically, four moderate categorized systems were selected, with 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, CLA selected the OIGNet from the total population of 17 OIG FISMA systems for testing. The OIGNet was selected based on risk since it is a moderate categorized system that supports FHFA-OIG applications that reside on the network. CLA tested the five systems' selected security controls to support its response to the FY 2022 Core IG FISMA Reporting Metrics.

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered 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.

STATUS OF PRIOR RECOMMENDATIONS

The table below summarize the status of our follow up related to the status of the open prior recommendations from the FY 2019 FISMA audit, FY 2019 Privacy audit, the FY 2020 FISMA audit, the FY 2021 Privacy audit, and the FY 2021 FISMA audit.[15]

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
AUD 2019-009, Finding # 3	We recommend that FHFA Privacy Office: 5. Determine privacy controls that are information system-specific, and/or hybrid controls.	We found that the prior year recommendation has been resolved. FHFA determined which privacy controls were system level or organizational common control.	**Closed**
	We recommend that FHFA Privacy Office: 6. Document privacy controls within each system's [System Security Plan] or system-specific privacy plan, clearly identifying whether controls are program level, common, information system-specific, or hybrid.	We found that the prior year recommendation has been resolved. FHFA determined which privacy controls were system level or organizational common control and has documented the controls in applicable system security plans as organizational common controls or system-specific.	**Closed**
AUD-2020-001, Finding # 2	We recommend FHFA Management: 6. Ensure investigations and reinvestigations of employees and contractors are performed in accordance with FHFA and Office of Personnel Management (OPM) standards, including applicable	We found that the prior year recommendation has been resolved. Background investigations and reinvestigations were conducted timely in accordance with OPM standards.	**Closed**

[15] Ibid. footnotes 5, 6, 7, 8, and 9.

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
	temporary measures prescribed by OPM if FHFA elects to defer reinvestigations.		
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. FHFA implemented a Privilege Access Management Tool to enhance its privileged identity management (PIM) and privileged access management (PAM) controls and program. However, FHFA divided the strategy and implementation of the Privilege Access Management Tool into 4 phases. Currently, FHFA is between phases 2 and 3 of the implementation plan.	**Open**
AUD 2021-001, Finding # 4	We recommend that FHFA management: 4. Ensure privacy-related policies and procedures are reviewed and kept up-to-date at least on a biennial basis in accordance with NIST SP 800-53, Revision 4. The review should be documented and annotated in the version history for each document to summarize any updates and/or no updates required, as applicable.	We found that the prior year recommendation has been resolved. FHFA privacy-related policies and procedures were reviewed and kept up-to-date at least on a biennial basis. The following policies and procedures have been reviewed: - *Use and Protection of Personally Identifiable Information Policy*, dated 5/10/2022. - *Guidelines on Disclosure of Information Contained in a Privacy Act System of Records*, dated 4/29/2022. - *Guidance on Amending or Correcting Records Contained in a FHFA System of Records*, dated 4/29/2022.	**Closed**

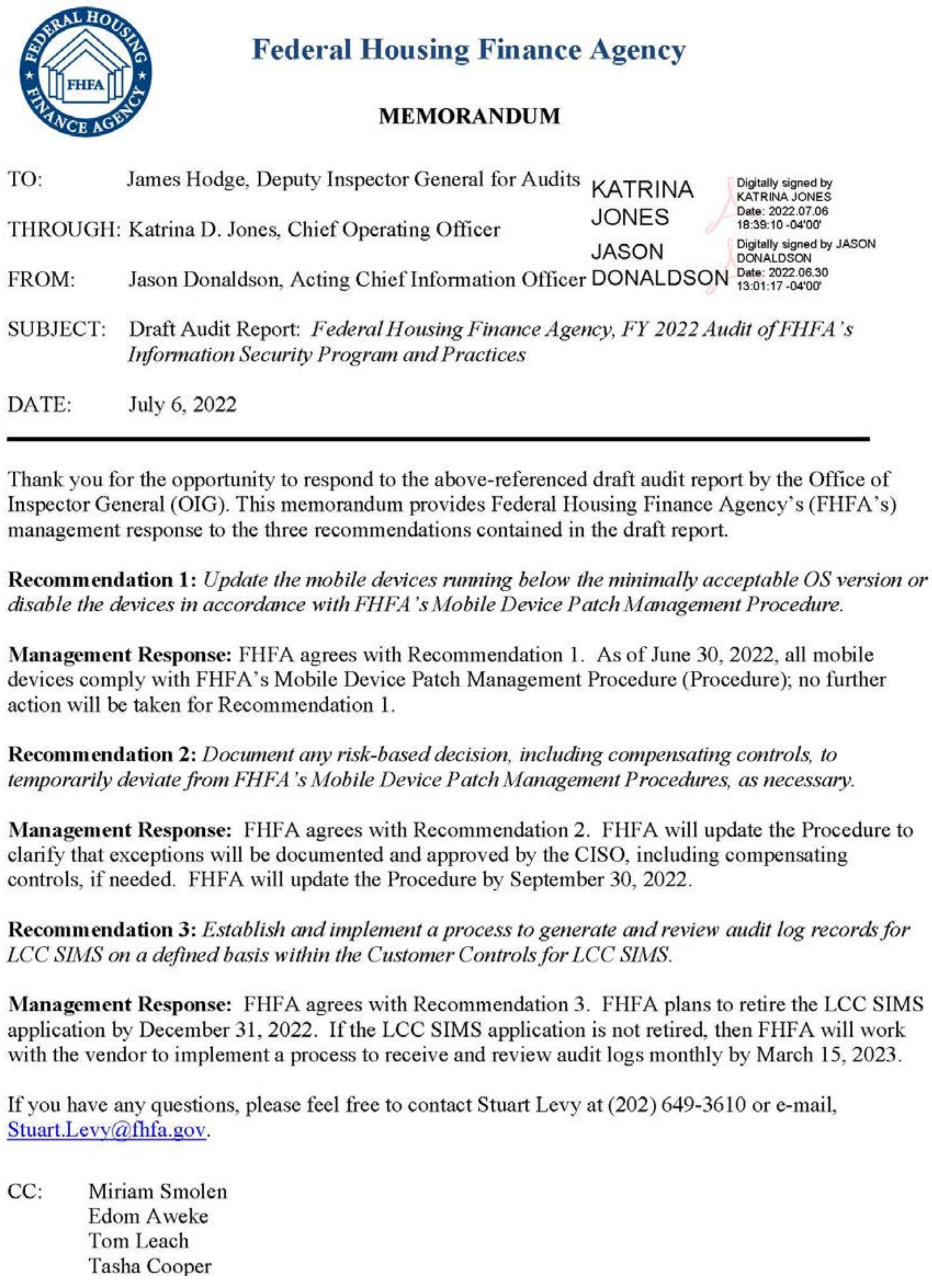
Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
		- *FHFA Incident and Breach Response Plan*, dated 9/1/2021. - *Update on Reducing Unnecessary Holdings of Personally Identifiable Information, Including Eliminating Unnecessary Use of Social Security Numbers*, dated 10/1/2021. - *Privacy Continuous Monitoring Strategy*, dated 5/2/2022. - *Privacy Impact Assessment Guide*, dated 4/29/2022. - *Privacy Program Plan*, dated 5/2/2022. - *Privacy Program Training Plan*, dated 4/29/2022. - *Procedures for Monitoring FHFA's Website for Compliance with FHFA's Website Privacy and Social Media Policies*, dated 4/29/2022. - *Procedures for Monitoring of Information Technology Systems that Contain Personally Identifiable Information*, dated 4/29/2022. - *Procedures for Updating and Maintaining an Inventory of Paper Holdings of Personally Identifiable Information*, dated 4/29/2022. - *Procedures on Drafting Privacy Act System of Records Notices*, dated 4/29/2022. - *Protecting Personally Identifiable Information (PII) When Teleworking,*	

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
		Working Remotely or Traveling, dated April 1, 2022.	
AUD 2021-001, Finding # 5	We recommend that FHFA management: 6. Assess, based on risk, the audit log records that should be forwarded to the Security Incident and Event Management (SIEM) tool for analysis and correlation.	We found that the prior year recommendation has been resolved. FHFA management assessed audit log records that should be forwarded to the SIEM tool for analysis and correlation. In addition, OTIM Security implemented Splunk Cloud to support the ingestion and processing of application logs currently processed by FHFA's Audit Central Database.	**Closed**
AUD 2021-011, Finding # 1	We recommend that FHFA management: 1. Update the Privacy Impact Analysis (PIAs) using the PIA Template for Affordable Housing Project (AHP), Federal Human Resources (FHR) Navigator, and Suspended Counter Party System (SCP).	We found that the prior year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of July 29, 2022.	**Open**
	We recommend that FHFA management: 2. Ensure PIAs are conducted timely using the PIA Template in accordance with the FHFA Privacy Program Plan (i.e., before a new system is developed, after a significant change to a system, or within three years of the PIA).	We found that the prior year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of July 29, 2022.	**Open**

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
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 not been resolved and remediation was in progress. Management provided an estimated completion date of July 29, 2022.	**Open**
AUD 2021-011, Finding # 3	We recommend that FHFA management: 4. Develop and implement privacy control assessment plans that include all required elements.	We found that the prior year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of July 29, 2022.	**Open**
	We recommend that FHFA management: 5. Ensure privacy control assessments are performed for all systems that collect PII.	We found that the prior year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of July 29, 2022.	**Open**
AUD 2022-001, Finding # 1	We recommend that FHFA management: 1. Ensure that Plan of Actions and Milestones (POA&M) items are generated for all known system security and privacy weaknesses in accordance with NIST SP 800-37, Revision 2, and *FHFA's POA&M Management Procedure*.	We found that the prior year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of September 30, 2022.	**Open**

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
AUD 2022-001, Finding # 3	We recommend that FHFA management: 2. Ensure that (a) the FHFA Information Security Incident and Personally Identifiable Information Breach Response Plan is reviewed and approved annually by the CISO and SAOP to include any new reporting guidelines from the United States Computer Emergency Readiness Team (US-CERT), changes to incident handling procedures based on lessons learned, and any new incident response developments throughout the year, and (b) documented evidence of that review and approval is maintained.	We found that the prior year recommendation has not been resolved and remediation was in progress. Management provided an estimated completion date of September 30, 2022.	**Open**
AUD 2022-001, Finding # 4	We recommend that FHFA management: 3. Ensure contingency training to staff with contingency related responsibilities is provided in accordance with the *FHFA Contingency Planning Standard.*	We found that the prior year recommendation has been resolved. FHFA management provided contingency training to staff with contingency related responsibilities in accordance with the *FHFA Contingency Planning Standard.*	**Closed**

FHFA’s MANAGEMENT COMMENTS



Federal Housing Finance Agency

MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audits

THROUGH: Katrina D. Jones, Chief Operating Officer

KATRINA JONES Digitally signed by KATRINA JONES Date: 2022.07.06 18:39:10 -04'00'

FROM: Jason Donaldson, Acting Chief Information Officer

JASON DONALDSON Digitally signed by JASON DONALDSON Date: 2022.06.30 13:01:17 -04'00'

SUBJECT: Draft Audit Report: *Federal Housing Finance Agency, FY 2022 Audit of FHFA’s Information Security Program and Practices*

DATE: July 6, 2022

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

Recommendation 1: *Update the mobile devices running below the minimally acceptable OS version or disable the devices in accordance with FHFA’s Mobile Device Patch Management Procedure.*

Management Response: FHFA agrees with Recommendation 1. As of June 30, 2022, all mobile devices comply with FHFA’s Mobile Device Patch Management Procedure (Procedure); no further action will be taken for Recommendation 1.

Recommendation 2: *Document any risk-based decision, including compensating controls, to temporarily deviate from FHFA’s Mobile Device Patch Management Procedures, as necessary.*

Management Response: FHFA agrees with Recommendation 2. FHFA will update the Procedure to clarify that exceptions will be documented and approved by the CISO, including compensating controls, if needed. FHFA will update the Procedure by September 30, 2022.

Recommendation 3: *Establish and implement a process to generate and review audit log records for LCC SIMS on a defined basis within the Customer Controls for LCC SIMS.*

Management Response: FHFA agrees with Recommendation 3. FHFA plans to retire the LCC SIMS application by December 31, 2022. If the LCC SIMS application is not retired, then FHFA will work with the vendor to implement a process to receive and review audit logs monthly by March 15, 2023.

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

CC: Miriam Smolen
Edom Aweke
Tom Leach
Tasha Cooper

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