

REDACTED

Federal Housing Finance Agency
Office of Inspector General



**Audit of the
Federal Housing Finance Agency's
Information Security Program,
Fiscal Year 2021**

This report contains redactions of information that is privileged or otherwise protected from disclosure under applicable law.

Audit Report • AUD-2022-001 • October 15, 2021



OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

October 15, 2021

TO: Kevin Smith, Chief Information Officer

FROM: Marla A. Freedman, Senior Audit Executive /s/

SUBJECT: Audit Report, *Audit of the Federal Housing Finance Agency's Information Security Program, Fiscal Year 2021* (AUD-2022-001)

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) 2021 independent evaluation of FHFA's 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 Department of Homeland Security's *FY 2021 Inspector General (IG) Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2021 IG FISMA Reporting Metrics), dated May 12, 2021. For this audit, CLA reviewed selected controls mapped to the FY 2021 IG FISMA Reporting 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 four findings: (1) Weaknesses with Plans of Action and

Milestones, (2) Weaknesses in FHFA's Privacy Program, (3) Weaknesses in FHFA's Incident Response Plan, and (4) Weaknesses in Contingency Training.

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 October 14, 2021, 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
Fiscal Year 2021



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

Fiscal Year 2021

Final Report



CliftonLarsonAllen LLP
CLAconnect.com

October 14, 2021

The Honorable Phyllis K. Fong
Acting Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024

Dear Acting Inspector General Fong:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the results of our audit of Federal Housing Finance Agency's (FHFA or Agency) information security program and practices for fiscal year 2021 in accordance with the Federal Information Security Modernization Act of 2014. We performed this audit under contract with the FHFA Office of Inspector General.

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,

A handwritten signature in black ink, appearing to read 'S. Mirzakhani'.

Sarah Mirzakhani, CISA
Principal



Acting Inspector General
Federal Housing Finance Agency

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Federal Housing Finance Agency's (FHFA or Agency) information security program and practices for fiscal year 2021 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 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 Department of Homeland Security's (DHS) *Fiscal Year (FY) 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2021 IG FISMA Reporting Metrics), dated May 12, 2021.

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 66 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 program and practices consistent with FISMA and reporting instructions issued by Office of Management and Budget (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 4, *Security and Privacy Controls for Federal 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 April 2021 to September 2021.

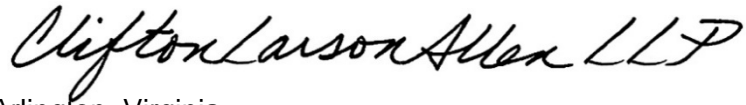
We concluded that FHFA implemented an effective information security program and complied with FISMA and related information security policies and procedures, standards, and guidelines by achieving an overall *Managed and Measurable* maturity level. Although FHFA implemented an effective information security program, its implementation of a subset of selected controls was not fully effective. Specifically, we noted weaknesses in four of the nine domains in the FY 2021

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

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

A handwritten signature in black ink that reads "CliftonLarsonAllen LLP". The signature is written in a cursive, flowing style.

Arlington, Virginia
October 14, 2021

Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program

Table of Contents

EXECUTIVE SUMMARY	1
Audit Results	2
AUDIT FINDINGS	5
1. Weaknesses with Plans of Action and Milestones.....	5
2. Weaknesses in FHFA's Privacy Program.....	6
3. Weaknesses in FHFA's Incident Response Plan	6
4. Weaknesses in Contingency Training	7
EVALUATION OF MANAGEMENT COMMENTS.....	9
APPENDIX I: BACKGROUND	10
APPENDIX II: OBJECTIVE, SCOPE, AND METHODOLOGY	13
APPENDIX III: STATUS OF PRIOR RECOMMENDATIONS	16
APPENDIX IV: FHFA'S MANAGEMENT COMMENTS	22

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

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 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's 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 Department of Homeland Security's (DHS) *Fiscal Year (FY) 2021 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2021 IG FISMA Reporting Metrics), dated May 12, 2021.

FY 2021 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 66 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*.

For this audit, CLA reviewed selected controls mapped to the FY 2021 IG FISMA Reporting Metrics for a sample of information systems³ 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.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA’s Information Security Program**

Audit Results

Progress Since FY 2020

At the beginning of FY 2021, there were 10 open recommendations from prior FISMA and Privacy audits (1 open recommendation from the FY 2019 FISMA audit,⁵ 2 open recommendations from the FY 2019 Privacy audit,⁶ and 7 open recommendations from the FY 2020 FISMA audit⁷). During 2021, we found that FHFA took corrective actions to address four open recommendations and we consider those recommendations closed. Corrective action is in progress on the other 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 2021 IG FISMA Reporting Metrics.

Table 1: Maturity Levels for FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Domain	Maturity
Identify	Risk Management	Level 3: Consistently Implemented
	Supply Chain Risk Management	Level 2: Defined ⁸
Protect Overall Protect Function Maturity Level: Level 4: Managed and Measurable	Configuration Management	Level 4: Managed and Measurable
	Identity and Access Management	Level 4: Managed and Measurable
	Data Protection and Privacy	Level 4: Managed and Measurable
	Security Training	Level 4: Managed and Measurable
Detect	Information Security Continuous Monitoring	Level 4: Managed and Measurable
Respond	Incident Response	Level 4: Managed and Measurable

⁵ 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.

⁶ FHFA-OIG Audit Report AUD-2019-009, *Audit of the Federal Housing Finance Agency’s 2019 Privacy Program*, issued August 28, 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 The FY 2021 IG FISMA Reporting Metrics indicated that in order to provide agencies with sufficient time to fully implement NIST Special Publication 800-53, Revision 5, in accordance with OMB A-130, these new metrics should not be considered for the purposes of the Identify framework function rating, and therefore should not be considered for the overall rating.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

Cybersecurity Framework Security Functions	Domain	Maturity
Recover	Contingency Planning	Level 3: Consistently Implemented
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 four of the nine domains of the FY 2021 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 2021 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Security Function	FY 2021 IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	Risk Management	Weaknesses with Plans of Action and Milestones (Finding 1)
	Supply Chain Risk Management	No weaknesses noted. ⁹
Protect	Configuration Management	No weaknesses noted.
	Identity and Access Management	No weaknesses noted.
	Data Protection and Privacy	Weaknesses in FHFA's Privacy Program (Finding 2)
	Security Training	No weaknesses noted.
Detect	Information Security Continuous Monitoring	No weaknesses noted.
Respond	Incident Response	Weaknesses in FHFA's Incident Response Plan (Finding 3)
Recover	Contingency Planning	Weaknesses in Contingency Training (Finding 4)

⁹ While FHFA has defined their Supply Chain Risk Management Plan, the plan was not finalized until nine months into the fiscal year. Therefore, it was not viable for FHFA to consistently implement controls in this domain for FY 2021. The required controls for Supply Chain Risk Management are prescribed in NIST SP 800-53, Revision 5, which was finalized in December 2020. In accordance with OMB A-130, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

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 Plans of Action and Milestones

Cybersecurity Framework Security Function: *Identify*
FY 2021 FISMA IG Reporting Metrics Domain: *Risk Management*

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

FHFA did not develop POA&Ms for all known security and privacy weaknesses in its information systems. Specifically, FHFA did not develop POA&M items for 11 recommendations made in 6 OIG audit reports to correct information system security and privacy weaknesses identified in 6 OIG audits.

An Office of Technology and Information Management (OTIM) Supervisory IT Specialist stated that the information system security and privacy weaknesses that were not tracked as POA&M items were tracked in another FHFA system. Accordingly, FHFA management did not believe it was necessary to track them as POA&M items.

NIST Special Publication (SP) 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Task A-6, Plan of Action and Milestones, requires federal agencies to prepare POA&Ms for security and privacy weaknesses in information systems, based on the findings and recommendations from audits, control assessments, and during continuous monitoring activities.

██ dated May 27, 2021, section 3.1.1, directs FHFA personnel to generate POA&M items from several sources: Security Assessment and Authorization, Incident Response Activities, Third Party Security Audits (e.g., OIG, Government Accountability Office), Vulnerability Scanning, Notification from Vendors, Help Desk Tickets, Management Risk Determination, and Continuous Monitoring.

Failure to track all known information system security and privacy weaknesses as POA&M items increases the risk that FHFA may not account for all known risks, and/or prioritize corrective actions. Additionally, this practice is contrary to NIST and FHFA requirements.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

We recommend that FHFA management:

Recommendation 1: *Ensure that POA&M items are generated for all known information system security and privacy weaknesses in accordance with NIST SP 800-37, Revision 2, and [REDACTED]*

2. Weaknesses in FHFA's Privacy Program

Cybersecurity Framework Security Function: *Protect*
FY 2021 IG FISMA Reporting Metrics Domain: *Data Protection and Privacy*

A 2021 CLA performance audit of FHFA's Privacy Program, performed under contract with FHFA-OIG,¹⁰ noted that although FHFA generally implemented comprehensive privacy and data protection policies and procedures, FHFA's implementation of certain privacy and data protection requirements was not fully achieved. Specifically, we noted weaknesses in FHFA's privacy impact assessments, privacy continuous monitoring strategy, privacy control assessment plans, and maintenance of privacy policies and procedures. As a result, we made five recommendations to assist FHFA in strengthening its privacy program.

This finding is included as a reference within this report since the FY 2021 IG FISMA Reporting Metrics includes the Data Protection and Privacy domain and therefore privacy controls were within the scope of the FISMA audit. However, we are not repeating the recommendations in this report. FHFA-OIG intends to follow-up on FHFA's corrective actions taken for those recommendations as part of the FY 2022 FISMA independent evaluation of FHFA's information security program and practices.

3. Weaknesses in FHFA's Incident Response Plan

Cybersecurity Framework Security Function: *Respond*
FY 2021 IG FISMA Reporting Metrics Domain: *Incident Response*

An incident response plan provides an organization with a roadmap for implementing its incident response capability, describes the structure and organization of the incident response capability, and provides a high-level approach for how to handle incidents.

FHFA's *Information Security Incident and Personally Identifiable Information Breach Response Plan* was not reviewed, updated, and approved annually. The last documented evidence of review was dated August 1, 2019.

An OTIM Supervisory IT Specialist asserted that the FHFA *Information Security Incident and Personally Identifiable Information Breach Response Plan* was reviewed in fiscal year 2020, but documented evidence of review and approval was not maintained.

Consistent with NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control Incident Response (IR)-8, the [REDACTED] requires the FHFA *Information Security*

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

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

Incident and Personally Identifiable Information Breach Response Plan to be reviewed, updated, and approved at least annually by the FHFA Chief Information Security Officer (CISO) and Senior Agency Official of Privacy (SAOP). The update should 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.

Failure to review and approve the incident response plan increases the risk that the FHFA *Information Security Incident and Personally Identifiable Information Breach Response Plan* may be outdated and changes that may impact the plan may not be implemented. Additionally, this practice is contrary to NIST and FHFA requirements.

We recommend that FHFA management:

Recommendation 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 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.*

4. Weaknesses in Contingency Training

Cybersecurity Framework Security Function: Recover
FY 2021 IG FISMA Reporting Metrics Domain: Contingency Planning

Contingency training provided by organizations should be commensurate to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. Training for contingency roles and responsibilities should reflect the specific continuity requirements in the contingency plan and may incorporate simulated events to facilitate an effective response by personnel in crisis situations.

FHFA did not provide contingency training to all agency users with contingency related responsibilities. Specifically, seven OTIM staff who have Systems Engineering core roles,¹¹ did not participate in the annual General Support System (GSS) disaster recovery training during the review period.

The Supervisory Information Technology Specialist stated that OTIM staff with contingency related responsibilities were mistakenly not included in the disaster recovery training in December 2020.

Consistent with NIST SP 800-53, Revision 4, control Contingency Planning (CP)-3, the [REDACTED] requires that FHFA provide contingency training to agency users with contingency related responsibilities (1) within the first year of assuming a contingency role or responsibility, (2) when required by agency system changes, and (3) annually thereafter.

¹¹The [REDACTED] page 5, details the OTIM personnel that constitute FHFA's primary and backup Systems Engineering core team responsible for maintaining FHFA's network and datacenter.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

Failure to provide contingency training to staff with contingency related responsibilities, as required by NIST and the FHFA standard, increases the risk that staff may not be adequately prepared to assume assigned roles and responsibilities during a real disaster. Further, FHFA relies heavily on its GSS IT infrastructure, and a risk that staff may not be prepared to assume assigned roles and responsibilities during a disaster could affect systems that rely on the GSS.

We recommend that FHFA management:

Recommendation 3: *Ensure contingency training to staff with contingency related responsibilities is provided in accordance with the* [REDACTED]

EVALUATION OF MANAGEMENT COMMENTS

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. FHFA's comments are included in Appendix IV.

For recommendation 1, FHFA management agrees with this recommendation, but they did not agree with the effect statement. FHFA stated that they do not agree with the statement that, "FHFA did not account for all risks." However, this statement as worded was not in this report. Based on discussions with FHFA management, this was paraphrased correlating to the statement, "increase the risk that FHFA may not account for all known risks, and/or prioritize corrective actions."

In a meeting subsequent to the issuance of the final draft of this report, FHFA's CISO confirmed FHFA's plan to implement recommendation 1, as written, by September 30, 2022. To the extent that FHFA has committed to ensure that POA&M items are generated for all known information system security and privacy weaknesses in accordance with NIST SP 800-37, Revision 2, and [REDACTED] we consider FHFA's planned corrective action to meet the intent of this recommendation.

For recommendation 2, FHFA updated and approved the *FHFA Information Incident and Breach Response Plan* on September 8, 2021. Based on our review of the updated plan, we consider this recommendation closed and implemented.

For recommendation 3, FHFA agrees with this recommendation. FHFA will ensure contingency training to staff with contingency related responsibilities is provided in accordance with the [REDACTED]. This action will be completed by September 30, 2022. We consider FHFA's planned corrective action to meet the intent of this recommendation.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

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 heads¹² 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.

¹² 44 USC § 3554, Federal agency responsibilities.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

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 DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On November 9, 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for Federal agencies to report to OMB and, where applicable, DHS. Accordingly, the FY 2021 IG FISMA Reporting Metrics provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security program.¹³

The FY 2021 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**.

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Domains in the FY 2021 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

¹³ Available online at <https://www.cisa.gov/publication/fy21-fisma-documents>.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

The foundational levels of the maturity model in the FY 2021 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** 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.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

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 DHS FY 2021 IG FISMA Reporting Metrics, dated May 12, 2021.

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 66 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for the following sample of three systems from the 30 systems in FHFA's FISMA inventory of information systems:

- Community Support Program (CSP)¹⁴
- Federal Human Resources (FHR) Navigator¹⁵
- FHFA GSS¹⁶

¹⁴CSP is used to collect, store, and review Community Support Statement information. CSP is a web-application with a public facing site that resides in the FHFA Demilitarized Zone (DMZ). FHFA users of CSP access the system through an internal web application.

¹⁵ FHR Navigator is an integrated web-based enterprise system that automates federal HR within a single platform. It is designed to automate federal HR administrative activities; manage different HR function tasks through an integrated system; accelerate and streamline typical HR processing steps, and support new government-wide hiring and workforce planning initiatives; and support services that HR offices deliver to employees, such as providing benefits administration services counseling and preparing retirement packages. The FHR Navigator system is for internal use only and does not post publicly accessible information.

¹⁶ 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.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

The audit also included an evaluation of whether FHFA took corrective action to address open recommendations from the FY 2019¹⁷ FISMA audit, FY 2019¹⁸ Privacy audit, and the 2020¹⁹ FISMA audit. The FY 2019 Privacy audit recommendations were followed up on during the FY 2021 Privacy audit²⁰ and are also referenced in this report.

Audit fieldwork covered FHFA headquarters located in Washington DC, from April 2021 to September 2021.

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 October 14, 2021. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 14, 2021.

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 and FY 2020. 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:

- Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*.
- FY 2021 IG FISMA Reporting Metrics.
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for specification of security controls.
- NIST SP 800-37, Revision 2, *Guide for Applying the Risk Management Framework to Federal Information Systems*, for the risk management framework controls.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, for the assessment of security control effectiveness.

¹⁷ Ibid. footnote 5.

¹⁸ Ibid. footnote 6.

¹⁹ Ibid. footnote 7.

²⁰ Ibid. footnote 10.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).
- FHFA policies and procedures, including but not limited to: [REDACTED]

CLA selected three FHFA systems from the total population of 30 FISMA reportable systems for testing. The three systems were selected based on risk. Specifically, three moderate categorized systems were selected, with one being the FHFA GSS that supports FHFA's applications that reside on the network, and the other two being systems that had not been tested in prior years. CLA tested the three systems' selected security controls to support its response to the FISMA IG 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.

Federal Housing Finance Agency
 FY 2021 Audit of FHFA’s Information Security Program

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, and the FY 2020 FISMA audit.²¹

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 not been resolved. FHFA has not designated whether each privacy control is a program management, common, system-specific, or hybrid control. Specifically, neither, the <i>FHFA Program Plan for Privacy</i> , nor system security plans (SSPs) for Affordable Housing Project (AHP), FHR Navigator, and Suspended Counterparty System (SCP) designated which privacy control is a program management, common, system-specific, or hybrid control. We noted that FHFA disagreed with this recommendation. However, FHFA committed to a course of action that met the intent of the recommendation. That action is to be completed within one year of the publication of Revision 5 to NIST SP 800-53. Revision 5, which was published December 10, 2020.	Open
	We recommend that FHFA Privacy Office:	We found that the prior year recommendation has not been resolved. Privacy controls were not documented within the SSPs for the	Open

²¹ Ibid. footnotes 5,6, and 7.

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
	<p>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.</p>	<p>FHFA information systems selected for testing:</p> <ul style="list-style-type: none"> • AHP • FHR Navigator • SCP <p>We noted that FHFA disagreed with this recommendation. However, FHFA committed to a course of action that met the intent of the recommendation. That action is to be completed within one year of the publication of Revision 5 to NIST SP 800-53. Revision 5, was published December 10, 2020.</p>	
<p>AUD-2020-001, Finding # 2</p>	<p>We recommend FHFA Management:</p> <p>6. Ensure investigations and reinvestigations of employees and contractors are performed in accordance with FHFA and Office of Personnel Management (OPM) standards, including applicable temporary measures prescribed by OPM if FHFA elects to defer reinvestigations.</p>	<p>We found that the prior year recommendation has not been resolved. In FY 2021, FHFA Office of Human Resource Management (OHRM) transitioned personnel security functions for the entire agency to the Department of Interior (DOI). DOI is continuing to work through the backlog of past-due background reinvestigations from the prior year. The estimated timeline to complete the backlogged reinvestigations is January 2022.</p>	<p>Open</p>
<p>AUD 2021-001, Finding # 1</p>	<p>We recommend that FHFA management:</p> <p>1. Update ██████████ in a risk-based manner.</p>	<p>We found that the prior year recommendation has been resolved. OTIM implemented the ██████████ which provides OTIM System Administrators guidance for performing ██████████ management. For updates identified by the</p>	<p>Closed</p>

Federal Housing Finance Agency
 FY 2021 Audit of FHFA's Information Security Program

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
		<p>[REDACTED] will notify users to update [REDACTED] within a specific timeframe. Users failing to comply [REDACTED] will have their [REDACTED] the user needs to contact the Help Desk to have [REDACTED]</p>	
	<p>We recommend that FHFA management:</p> <p>2. Develop and implement a process to ensure that [REDACTED] and updated in a timely manner.</p>	<p>We found that the prior year recommendation has been resolved. OTIM implemented the [REDACTED] which provides OTIM System Administrators guidance for performing [REDACTED] For updates identified by the [REDACTED] will notify users to update their [REDACTED] within a specific timeframe. Users failing to comply [REDACTED] will have their [REDACTED] the user needs to contact the Help Desk to have [REDACTED]</p>	<p>Closed</p>
<p>AUD 2021-001, Finding #3</p>	<p>We recommend that FHFA management:</p> <p>3. Implement the planned [REDACTED]</p>	<p>We found that the prior year recommendation has not been resolved. FHFA did not enforce [REDACTED] While FHFA does enforce [REDACTED]</p>	<p>Open</p>

Federal Housing Finance Agency
 FY 2021 Audit of FHFA's Information Security Program

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
	<p>[REDACTED]</p>	<p>[REDACTED]</p> <p>FHFA Management stated that they are in the final procurement stages of acquiring a solution. Management anticipates having a strategy by September 2021, with implementation to follow in FY 2022.</p>	
<p>AUD 2021-001, Finding #4</p>	<p>We recommend that FHFA management:</p> <p>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.</p>	<p>We found that the prior year recommendation has not been resolved. The following policies and procedures have not been updated in accordance with NIST SP 800-53 Revision 4:</p> <p>[REDACTED]</p>	<p>Open</p>
<p>AUD 2021-001, Finding #5</p>	<p>We recommend that FHFA management:</p> <p>5. Complete the process of forwarding [REDACTED]</p>	<p>We found that the prior year recommendation has been resolved. OTIM implemented the [REDACTED] Tool which forwards three types of [REDACTED]</p> <p>[REDACTED]</p>	<p>Closed</p>

**Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program**

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
	<p>We recommend that FHFA management:</p> <p>6. Assess, based on risk, the [REDACTED] that should be forwarded to [REDACTED]</p>	<p>[REDACTED]</p> <p>We found that the prior year finding has not been resolved. FHFA did not [REDACTED] to increase organization-wide situational awareness. Specifically, we noted: [REDACTED] were not sent to [REDACTED] FHFA used other tools [REDACTED] FHFA did not have a defined process to [REDACTED]</p> <p>FHFA is expanding the use of a newly procured [REDACTED]. The new [REDACTED] is planned for implementation by the end of September 2021. As such, in FY 2022, FHFA is planning on incorporating [REDACTED] from additional [REDACTED] into their [REDACTED] by December 2021.</p>	<p>Open</p>
<p>AUD 2021-001, Finding #6</p>	<p>We recommend that FHFA management:</p> <p>7. Ensure that the Continuity of Operations Plan (COOP) and associated documentation is reviewed annually to identify any required updates or changes, and ensure identified updates and changes are made. Records of</p>	<p>We found that the prior year recommendation has been resolved. The COOP was last updated on September 29, 2020.</p>	<p>Closed</p>

Federal Housing Finance Agency
 FY 2021 Audit of FHFA's Information Security Program

Report #/ Finding #	Recommendation	FHFA Actions Taken	Auditor's Position on Status
	changes should be recorded in the document.		

Federal Housing Finance Agency
 FY 2021 Audit of FHFA's Information Security Program

FHFA's MANAGEMENT COMMENTS



Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Senior Audit Executive

KEVIN
SMITH

Digitally signed by KEVIN
SMITH
Date: 2021.09.27
13:42:37 -04'00'

FROM: Kevin Smith, Chief Information Officer

SUBJECT: Draft Audit Report: *Federal Housing Finance Agency, FY 2021 Audit of FHFA's Information Security Program*

DATE: September 22, 2021

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: *Ensure that POA&M items are generated for all known information system security and privacy weaknesses in accordance with NIST SP 800-37, Revision 2, and [REDACTED]*

Management Response:

FHFA agrees with Recommendation 1, however, we do not agree with the statement, "that FHFA did not account for all risks." FHFA tracks OIG and GAO audit findings and coordinates remedial actions and completion dates with applicable stakeholders. Audit findings are tracked and coordinated by OTIM's Compliance, Audit and Enterprise Architecture group, which serves as OTIM's primary liaison to OIG and GAO auditors. Therefore, tracking these findings separately from FHFA's POA&Ms did not "increase the risk that FHFA may not account for all known risks, and/or prioritize corrective actions" as all audit findings are tracked, communicated and remediated in a timely manner as demonstrated by FHFA's progress in closing prior recommendations described in Appendix III. FHFA will review, evaluate, and modify the POA&M process as necessary to ensure that all risks are being centrally tracked. This action will be completed by September 30, 2022.

Recommendation 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 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.*

Federal Housing Finance Agency
FY 2021 Audit of FHFA's Information Security Program

September 22, 2021

Page 2 of 2

Management Response: FHFA agrees with Recommendation 2. On September 1, 2021, FHFA updated the Plan, now referred to as the *FHFA Information Incident and Breach Response Plan*, which was posted to the FHFA Intranet on September 14, 2021. FHFA believes that this action is responsive to Recommendation 2 and considers it remediated.

Recommendation 3: *Ensure contingency training to staff with contingency related responsibilities is provided in accordance with the [REDACTED]*

Management Response: FHFA agrees with Recommendation 3. FHFA will ensure contingency training to staff with contingency related responsibilities is provided in accordance with the [REDACTED]. The training will be completed by September 30, 2022.

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

CC: Edom Aweke
Tom Leach
Tasha Cooper
Ralph Mosios
John Major

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaog.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.fhfaog.gov/ReportFraud
- Write:

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