Federal Housing Finance Agency
Office of Inspector General

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

Audit Report • AUD-2022-002 • October 15, 2021

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

October 15, 2021

TO: Michael Smith, Chief Information Officer

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

SUBJECT: Audit Report, *Audit of the Federal Housing Finance Agency Office of Inspector General's Information Security Program and Practices, Fiscal Year 2021* (AUD-2022-002)

We are pleased to transmit the subject report.

The Federal Information Security Modernization Act of 2014 (FISMA) requires the Federal Housing Finance Agency Office of Inspector General (OIG) 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 OIG's information security program as a performance audit under generally accepted government auditing standards. The objectives of this audit were to (1) evaluate the effectiveness of OIG's information security program and practices, including OIG'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, 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 OIG's FISMA system inventory.

Based on its audit work, CLA concluded that OIG generally 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 OIG implemented an effective information security program, its implementation of a control was not fully effective. Specifically, CLA reported one

finding related to weaknesses with background investigations. However, that weakness is being addressed by OIG management. CLA made no recommendation.

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 OIG'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.

Attachment

ATTACHMENT

Audit of the Federal Housing Finance Agency
Office of Inspector General's
Information Security Program
Fiscal Year 2021

Audit of the Federal Housing Finance Agency Office of Inspector General'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 Office of Inspector General's (FHFA-OIG) 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-OIG.

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

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Acting Inspector General
Federal Housing Finance Agency

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Federal Housing Finance Agency Office of Inspector General's (FHFA-OIG) information security program and practices for fiscal year (FY) 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-OIG's information security program and practices, including FHFA-OIG's compliance with FISMA and related information security policies, procedures, standards, and guidelines; and (2) respond to the Department of Homeland Security's (DHS) *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-OIG'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-OIG's FISMA inventory of information systems.

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

We concluded that FHFA-OIG 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.

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

Although FHFA-OIG implemented an effective information security program, its implementation of a control was not fully effective. Specifically, we noted a weakness in one of the nine domains in the FY 2021 IG FISMA Reporting Metrics. However, that weakness is being addressed. Accordingly, we are not making a recommendation.

Additional information on our finding is included in the accompanying report.

CliftonLarsonAllen LLP

Arlington, Virginia
October 14, 2021

Table of Contents

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-OIG's information security program and practices.

The objectives of this performance audit were to (1) evaluate the effectiveness of the FHFA-OIG's information security program and practices, including FHFA-OIG'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-OIG'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 supporting FHFA-OIG's General Support System (GSS), OIGNet. The system was selected from the total population of 17 systems[3] in FHFA-OIG'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-OIG's FISMA inventory of information systems details a list of FHFA-OIG's FISMA reportable systems.

Audit Results

Progress Since 2020

The prior year FHFA-OIG FISMA audit report[5] noted one finding that upon notification, FHFA-OIG took corrective action and corrected the weakness. Therefore, there were no open prior year recommendations.

Current Status

We concluded that FHFA-OIG 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	Domains	Maturity
Identify	**Risk Management**	Level 5: Optimized
	Supply Chain Risk Management	Level 2: Defined[6]
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
Recover	**Contingency Planning**	Level 4: Managed and Measurable
Overall		**Level 4: Managed and Measurable (Effective)**

[5] FHFA-OIG Audit Report AUD-2021-002, *Audit of the Federal Housing Finance Agency Office of the Inspector General's Information Security Program Fiscal Year 2020*, issued October 20, 2020.

[6] 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.

Although we concluded that FHFA-OIG implemented an effective information security program, its implementation of a control was not fully effective. We noted a weakness in one of the nine IG FISMA Metric Domains (**see Table 2**). However, that weakness is being addressed. Accordingly, we are not making a recommendation. In response to a draft of this report, FHFA-OIG acknowledged that the report contained no recommendations, and the OIG took action to address the weakness noted.

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**	No weaknesses noted.
	Supply Chain Risk Management	No weaknesses noted.[7]
Protect	**Configuration Management**	No weaknesses noted.
	Identity and Access Management	Weaknesses with Background Investigations (**Finding 1**)
	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 finding. Appendix I provides background information on FISMA. Appendix II describes the audit objectives, scope, and methodology. Appendix III includes FHFA-OIG's management comments.

[7] While FHFA-OIG has defined their Supply Chain Risk Management Plan, the plan was not finalized until six months into the fiscal year. Therefore, it was not viable for FHFA-OIG 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.

AUDIT FINDING

1. Weaknesses with Background Investigations

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Reporting Metrics Domain: *Identity and Access Management*

The background investigation process is used to verify an individual's reliability and trustworthiness through checking and confirming someone's criminal record, education, employment history, and other activities from their past. In this context, background reinvestigations are to be conducted on fixed cycles based on risk for current government employees and contractors to establish their continued suitability for employment.

Based on a review of the fiscal year (FY) 2021 background investigation tracking report and confirmation from the FHFA-OIG management, we found that 42 of 152 FHFA-OIG employees and contractors' background reinvestigations were overdue (i.e., not completed on a five-year reinvestigation cycle) in accordance with Office of Personnel Management (OPM) guidance. Specifically, we noted:

- 37 employees' reinvestigations were overdue; and
- 5 contractors' reinvestigations were overdue.

According to the FHFA-OIG Human Resources (HR) Director, in FY 2021 FHFA's Office of Human Resource Management (OHRM) transitioned personnel security functions for the entire agency, including FHFA-OIG, to the Department of Interior (DOI). In preparation for the transition, FHFA-OIG provided the information necessary to initiate the required reinvestigations to a FHFA Personnel Security Specialist to transmit to DOI, in July 2020. As of October 2020, FHFA-OIG assumed responsibility for providing personal identification information and position designation records, as necessary, to DOI to conduct their FHFA-OIG's personnel security functions. The FHFA-OIG HR Director stated and provided documentary evidence that the backlogged reinvestigations were late at the time FHFA-OIG assumed this responsibility, but all have been initiated by DOI and are in progress.

The FHFA-OIG *General Support System (OIGNet) System Security Plan (SSP) & Control Implementation Procedures,* dated March 30, 2021, Personnel Security (PS)-3 control, requires individuals to be reinvestigated according to OPM guidance.[8]

OPM's regulation at 5 Code of Federal Regulation (C.F.R) part 731.106, requires agencies to submit and adjudicate public trust reinvestigations at least once every five years.

Without timely reinvestigations of FHFA-OIG employees and contractors, FHFA-OIG lacks assurance that employees and contractors remain suitable for employment.

Based on the actions taken by FHFA-OIG and DOI to initiate the backlogged reinvestigations, we make no recommendation for this finding. Going forward, we encourage FHFA-OIG, in coordination with DOI, to ensure reinvestigations of FHFA-OIG employees and contractors are scheduled and monitored so that the reinvestigations are completed timely in accordance with FHFA-OIG *OIGNet SSP & Control Implementation Procedures* and OPM regulation 5 C.F.R. part 731.106 (i.e., within five years for public trust reinvestigations).

[8] This was also a requirement in the 2020 SSP.

EVALUATION OF MANAGEMENT COMMENTS

In response to a draft of this report, FHFA-OIG acknowledged that the report contained no recommendations, and the OIG took action to address the weakness noted. FHFA-OIG's comments are included in Appendix III.

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.

The FHFA-OIG was established in 2010. Its mission is to promote the economy, efficiency, and effectiveness of FHFA's programs; prevent and detect fraud, waste, and abuse in FHFA's programs; and seek sanctions and prosecutions against those who are responsible for such fraud, waste, and abuse. To support its mission, FHFA-OIG operates its own desktops, servers, and network infrastructure separate from FHFA.

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[9] 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.

[9] 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 Special Publications (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.[10]

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

[10] Available online at https://www.cisa.gov/publication/fy21-fisma-documents.

Federal Housing Finance Agency Office of Inspector General
FY 2021 Audit of FHFA-OIG'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.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objectives of this performance audit were to: (1) evaluate the effectiveness of the FHFA-OIG's information security program and practices, including FHFA-OIG'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-OIG's information security program and practices 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*, over FHFA-OIG's GSS, OIGNet. The system was selected from the total population of 17 FHFA-OIG systems.

The audit also included a follow up on any prior FY 2020 FISMA audit[11] recommendations to determine if FHFA-OIG made progress in implementing the recommended improvements concerning its information security program. Upon follow-up, CLA noted there were no recommendations for the FY 2020 FISMA audit.

Audit fieldwork covered FHFA-OIG's 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-OIG 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.

[11] Ibid. footnote 5.

Methodology

To determine if FHFA-OIG implemented an effective information security program, CLA conducted interviews with FHFA-OIG 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-OIG'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-OIG's information technology 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.

Our work in support of the audit was guided by applicable FHFA-OIG 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.
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).
- OPM's regulation at 5 C.F.R part 731.106.

CLA selected OIGNet from the total population of 17 OIG 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 OIGNet's 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.

FHFA-OIG's MANAGEMENT COMMENTS

OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

September 28, 2021

TO: Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP

THRU: John Sutherland, Deputy Inspector General for Administration (Acting)

FROM: Michael Smith, Chief Information Officer

SUBJECT: Management Response to CliftonLarsonAllen's Performance Audit of FHFA-OIG's Security Program

Thank you for the opportunity to respond to CliftonLarsonAllen's Fiscal Year 2021 FISMA Audit (Audit) of the Federal Housing Finance Agency, Office of Inspector General (FHFA-OIG). We appreciate the opportunity to comment on the draft report, dated September 15, 2021, which contained a single finding. CliftonLarsonAllen found that FHFA-OIG has taken the appropriate actions for this finding, and therefore the draft report contained no recommendations.

As noted in the draft report, the overdue background reinvestigations associated with the identified finding were late at the time FHFA-OIG assumed responsibility for the reinvestigation process from FHFA, but all have been initiated by DOI and are currently in progress. FHFA-OIG, in coordination with DOI, will continue to ensure reinvestigations of FHFA-OIG employees and contractors are scheduled and monitored so that the reinvestigations are completed timely in accordance with OPM regulations.

We trust that the results of this independent audit will provide assurance to our stakeholders that FHFA-OIG's Information Security Program and practices are operating effectively in compliance with FISMA legislation, OMB guidance, and NIST Special Publications. These independent audit results confirm that our Information Technology (IT) infrastructure, policies, procedures and practices are suitably designed and implemented to provide reasonable assurance of adequate security.

We appreciate CliftonLarsonAllen's professionalism in conducting FHFA-OIG's Fiscal Year 2021 FISMA audit.

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