

Federal Housing Finance Agency
Office of Inspector General



**Audit of the Federal Housing
Finance Agency's Information
Security Programs and Practices
Fiscal Year 2023**

Audit Report • AUD-2023-004 • July 26, 2023



OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

July 26, 2023

TO: Tammy Tippie, 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 Programs and Practices Fiscal Year 2023* (AUD-2023-004)

We are pleased to transmit the subject report.

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

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

Based on the selected controls and the sampled information systems reviewed, CLA concluded that collectively the Agency's information security programs and practices were effective 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. Although the Agency implemented effective information security programs and practices, a subset of selected controls was not fully effective. Specifically, CLA reported seven findings: (1) Weaknesses in FHFA's Supply Chain Risk Management Controls; (2) Weaknesses in FHFA-

OIG's Supply Chain Risk Management Controls; (3) Weaknesses in FHFA's Vulnerability Management; (4) Weaknesses in FHFA's Event Logging Maturity; (5) Weaknesses in FHFA-OIG Event Logging Maturity; (6) Weaknesses in FHFA's Incident Response Plans and Procedures; and (7) Weaknesses in FHFA's Contingency Plan Testing. To address these weaknesses, CLA made 10 recommendations and reaffirmed two recommendations from a prior OIG audit.

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 the Agency's implementation of its information security programs and practices and compliance with FISMA and related information security policies, procedures, standards, and guidelines. CLA is responsible for the attached auditor's report dated July 13, 2023, 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, the Agency's management agreed with the recommendations made in the report and outlined its plans to address them.

Attachment

ATTACHMENT

Audit of the Federal Housing Finance Agency's
Information Security Programs and Practices,
Fiscal Year 2023

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

Fiscal Year 2023

Final Report



CPAs | CONSULTANTS | WEALTH ADVISORS

[CLAconnect.com](https://www.CLAconnect.com)



CliftonLarsonAllen LLP
CLAconnect.com

July 13, 2023

The Honorable Brian M. 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 the Federal Housing Finance Agency's (FHFA) and the FHFA Office of Inspector General's (FHFA-OIG's) information security programs and practices for fiscal year 2023 in accordance with the Federal Information Security Modernization Act of 2014. Our report presents FHFA's and FHFA-OIG's combined results (collectively referred to as the Agency). We performed this audit under contract with the FHFA-OIG.

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

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

Very truly yours,

A handwritten signature in cursive script, appearing to read 'S. 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) and FHFA Office of Inspector General's (FHFA-OIG), collectively referred to as the Agency for reporting combined results, information security programs and practices for fiscal year 2023 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 and practices. The Act also requires Inspectors General (IG) to conduct an annual independent evaluation of their agencies' information security programs and practices.

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

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

For this year's review, IGs were required to assess 20 Core IG FISMA Reporting Metrics and 20 Supplemental IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area.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 the Agency's information security programs and practices consistent with FISMA and reporting instructions issued by the Office of Management and Budget (OMB). The scope also included assessing selected 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 the Agency's FISMA inventory of information systems.

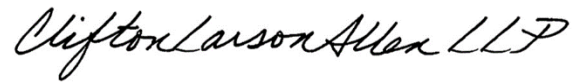
The scope of this performance audit covered the Agency's information security programs and practices from April 1, 2022, through March 31, 2023. We conducted audit fieldwork remotely from October 2022 through June 2023.

¹ The function areas are further broken down into nine domains (Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning).

We concluded that collectively the Agency's information security programs and practices were effective 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. Although the Agency implemented effective security programs and practices, a subset of selected controls was not fully effective. Specifically, we noted weaknesses in four of the nine domains in the FY 2023 IG FISMA Reporting Metrics. As such, we made 10 new recommendations and reaffirmed two prior recommendations from a prior OIG audit² to assist the Agency in strengthening its information security programs and practices.

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

CliftonLarsonAllen LLP

A handwritten signature in cursive script that reads "CliftonLarsonAllen LLP".

Arlington, Virginia
July 13, 2023

² 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)* (December 13, 2021).

**Federal Housing Finance Agency
FY 2023 Audit of FHFA’s Information Security Programs and Practices**

Table of Contents

| | |
|--|-----------|
| EXECUTIVE SUMMARY | 1 |
| Audit Results | 2 |
| AUDIT FINDINGS..... | 6 |
| 1. Weaknesses in FHFA’s Supply Chain Risk Management Controls..... | 6 |
| 2. Weaknesses in FHFA-OIG’s Supply Chain Risk Management Controls..... | 11 |
| 3. Weaknesses in FHFA’s Vulnerability Management..... | 15 |
| 4. Weaknesses in FHFA’s Event Logging Maturity..... | 16 |
| 5. Weaknesses in FHFA-OIG’s Event Logging Maturity..... | 19 |
| 6. Weaknesses in FHFA’s Incident Response Plans and Procedures | 21 |
| 7. Weaknesses in FHFA’s Contingency Plan Testing | 23 |
| EVALUATION OF MANagements’ COMMENTS | 25 |
| APPENDIX I: BACKGROUND | 27 |
| APPENDIX II: OBJECTIVE, SCOPE, AND METHODOLOGY | 30 |
| APPENDIX III: STATUS OF PRIOR RECOMMENDATIONS | 34 |
| APPENDIX IV: MANagements’ COMMENTS | 38 |

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 (IGs) to assess the effectiveness of their agency's information security program and practices. The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

The Federal Housing Finance Agency Office of Inspector General (FHFA-OIG) engaged 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 (collectively referred to as the Agency for reporting combined results) information security programs and practices for fiscal year (FY) 2023. The objectives of this performance audit were to (1) evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines; and (2) respond to the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2023 IG FISMA Reporting Metrics).³

The scope of this performance audit covered the Agency's information security programs and practices from April 1, 2022, through March 31, 2023. We conducted audit fieldwork remotely from October 2022 through June 2023.

The FY 2023 IG FISMA Reporting Metrics requires us to assess the maturity of five functional areas in the Agency's information security programs and practices. For this year's review, IGs were required to assess 20 Core⁴ IG FISMA Reporting Metrics and 20 Supplemental⁵ IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area.⁶ The maturity levels are Level 1 – *Ad Hoc*, Level 2 – *Defined*, Level 3 – *Consistently Implemented*, Level 4 – *Managed and Measurable*, and Level 5 – *Optimized*. To be considered effective, an agency's information security program must be rated Level 4 – *Managed and Measurable*. See Appendix I for additional information on the FY 2023 IG FISMA Reporting Metrics and FISMA reporting requirements.

For this audit, CLA reviewed selected controls from NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2023 IG FISMA Reporting Metrics for a sample of information systems⁷ in the Agency's FISMA inventories of reportable information systems.

³ See FY 2023 IG FISMA Reporting Metrics online [here](#).

⁴ Core Metrics are assessed annually and represent a combination of Administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.

⁵ Supplemental Metrics are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

⁶ The function areas are further broken down into nine domains.

⁷ According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Federal Housing Finance Agency
FY 2023 Audit of FHFA’s Information Security Programs and Practices

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

Progress Since FY 2022

At the beginning of FY 2023, there were 11 open recommendations from prior FISMA and Privacy audits (one open recommendation from the FY 2020 FISMA audit,⁸ five open recommendations from the FY 2021 Privacy audit,⁹ two open recommendations from the FY 2021 FISMA audit,¹⁰ and three open recommendations from FY 2022 FISMA Audit).¹¹ During the audit, we found that FHFA took corrective actions to address nine recommendations and we consider those recommendations closed. Corrective actions are in progress on the other two open recommendations. Refer to Appendix III for a detailed description of the status of each recommendation.

Current Status

We concluded that collectively the Agency’s information security programs and practices were effective 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 2023 IG FISMA Reporting Metrics.

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

⁹ FHFA-OIG Audit Report AUD-2021-011, *Audit of the Federal Housing Finance Agency’s 2021 Privacy Program* (August 11, 2021).

¹⁰ FHFA-OIG Audit Report AUD-2022-001, *Audit of the Federal Housing Finance Agency’s Information Security Program Fiscal Year 2021* (October 15, 2021).

¹¹ FHFA-OIG Audit Report 2022-009, *Audit of the Federal Housing Finance Agency’s Information Security Program and Practices Fiscal Year 2022* (July 28, 2022).

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

Table 1: Maturity Levels for FY 2023 IG FISMA Reporting Metrics

| Cybersecurity Framework Security Functions | Domain | Maturity |
|---|--|---|
| Identify <i>Overall Identify Function Maturity Level: Level 4: Managed and Measurable</i> | Risk Management | Level 4: <i>Managed and Measurable</i> |
| | Supply Chain Risk Management | Level 3: <i>Consistently Implemented</i> |
| Protect <i>Overall Protect Function Maturity Level: Level 4: Managed and Measurable</i> | Configuration Management | Level 3: <i>Consistently Implemented</i> |
| | Identity and Access Management | Level 4: <i>Managed and Measurable</i> |
| | Data Protection and Privacy | Level 2: <i>Defined</i> |
| | Security Training | Level 5: <i>Optimized</i> |
| Detect <i>Overall Detect Function Maturity Level: Level 4: Managed and Measurable</i> | Information Security Continuous Monitoring | Level 4: <i>Managed and Measurable</i> |
| Respond <i>Overall Respond Function Maturity Level: Level 3: Consistently Implemented</i> | Incident Response | Level 3: <i>Consistently Implemented</i> |
| Recover <i>Overall Recover Function Maturity Level: Level 3: Consistently Implemented</i> | Contingency Planning | Level 3: <i>Consistently Implemented</i> |
| Overall | | Level 4: <i>Managed and Measurable (Effective)</i> |

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

In accordance with the FY 2023 IG FISMA Reporting Metrics guidance,¹² we focused on the calculated average of the Core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average of the Supplemental IG FISMA Reporting Metrics and progress made addressing outstanding prior year recommendations, to come to this risk-based conclusion. Further, we noted that three out of five Cybersecurity Functions were rated at Level 4 - *Managed and Measurable*. As a result, the Agency's overall maturity was rated as Level 4 - *Managed and Measurable* (Effective).¹³ The weaknesses we identified during this year's audit, in combination, did not significantly impact the Agency's overall information security programs and practices for us to consider it ineffective.

Although the Agency implemented effective information security programs and practices, a subset of selected controls was not fully effective. We noted weaknesses in four of the nine domains of the FY 2023 IG FISMA Reporting Metrics (see **Table 2**). As such, we made 10 new recommendations and reaffirmed two prior recommendations from a prior OIG audit¹⁴ to assist the Agency in strengthening its information security programs and practices. In a response to a draft of this report, FHFA and FHFA-OIG provided separate management responses related to their specific findings and recommendations. FHFA and FHFA-OIG management agreed with all 10 recommendations made in this report and outlined their plans to address each recommendation.

¹² The FY 2023 IG FISMA Reporting Metrics provided the agency IG the discretion to determine the rating for each of the Cybersecurity Framework domains and functions and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FISMA audit. Using this approach, IGs may determine that a particular domain, function area, or agency's information security program is effective at a calculated maturity lower level than level 4.

¹³ The FY 2023 IG FISMA Reporting Metrics were provided as a separate deliverable. The FY 2023 IG FISMA Reporting Metrics deliverable included calculated averages for the FY 2023 Core IG FISMA Reporting Metrics and Supplemental IG FISMA Reporting Metrics.

¹⁴ See footnote 2.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

Table 2: Weaknesses Noted in FY 2023 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2023 IG FISMA Reporting Metrics

| Cybersecurity Framework Security Function | FY 2023 IG FISMA Reporting Metrics Domain | Weaknesses Noted |
|---|---|--|
| Identify | Risk Management | No weaknesses noted. |
| | Supply Chain Risk Management | Weaknesses in FHFA's Supply Chain Risk Management Controls (Finding 1) Weaknesses in FHFA-OIG's Supply Chain Risk Management Controls (Finding 2) |
| Protect | Configuration Management | Weaknesses in FHFA's Vulnerability Management (Finding 3) |
| | Identity and Access Management | No weaknesses noted. |
| | Data Protection and Privacy | No weaknesses noted. |
| | Security Training | No weaknesses noted. |
| Detect | Information Security Continuous Monitoring | No weaknesses noted. |
| Respond | Incident Response | Weaknesses in FHFA's Event Logging Maturity (Finding 4) Weaknesses in FHFA-OIG's Event Logging Maturity (Finding 5) Weaknesses in FHFA's Incident Response Plans and Procedures (Finding 6) |
| | | |
| | | |
| Recover | Contingency Planning | Weaknesses in FHFA's Contingency Plan Testing (Finding 7) |

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

AUDIT FINDINGS

1. Weaknesses in FHFA's Supply Chain Risk Management Controls

Cybersecurity Framework Security Function: *Identify*

FY 2023 IG FISMA Reporting Metrics Domain: *Supply Chain Risk Management*

As required by the OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022), we found that FHFA created an inventory of "critical software"¹⁵ within 90 days or by December 13, 2022.

Contrary to OMB M-22-18, FHFA did not perform the appropriate planning to integrate the NIST Guidance¹⁶ into its software evaluation process (i.e., FHFA's *Supply Chain Risk¹⁷ Management Strategy* document) within 120 days or by January 12, 2023. Based on our review of FHFA's *Supply Chain Risk Management Strategy*, FHFA did not develop a process to communicate relevant secure software development requirements to vendors that include the following requirements:

- (1) Obtaining from software producers a "conformance statement" (i.e., a self-attestation letter) attesting their software development processes follow secure software development practices;
- (2) Obtaining from software producers artifacts that demonstrate conformance to secure software development practices, as needed; and
- (3) Establishing a system to store self-attestation letters available from software producers that are not publicly in a central location.

Additionally, an FHFA official stated that FHFA did discuss the need for developing training for reviewing and validating self-attestation letters within 180 days or by March 13, 2023, in accordance with OMB M-22-18. However, evidence of this discussion was not documented.

Overall, we found that FHFA did not request from OMB an extension or a waiver, nor document a plan for mitigating any potential risk, for not complying with some of the requirements of OMB M-22-18.

Office of Technology and Information Management (OTIM) officials stated that they plan to update FHFA's *Supply Chain Risk Management Strategy* to include the OMB M-22-18 requirements. Also, OTIM officials stated that updating FHFA's *Supply Chain Risk Management Strategy* requires discussions with multiple FHFA parties and offices to get a consensus on the updated language within FHFA's *Supply Chain Risk Management Strategy*. At the time of this audit,

¹⁵ NIST defines the term "critical software" as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: (a) is designed to run with elevated privilege or manage privileges; (b) has direct or privileged access to networking or computing resources; (c) is designed to control access to data or operational technology; (d) performs a function critical to trust; or (e) operates outside of normal trust boundaries with privileged access. According to NIST, the definition applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) that is purchased for, or deployed in, information systems and used for operational purposes.

¹⁶ The NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* (February 2022) and the NIST's *Software Supply Chain Security Guidance* under *EO 14028 Section 4e* (February 4, 2022) (these two documents are referred to as NIST Guidance) includes a set of practices that create the foundation for developing secure software.

¹⁷ Supply chain risk refers to the potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services, according to NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (May 2022).

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

discussions about the process of communicating relevant requirements for acceptable self-attestation letters to vendors and the collection of the letters in a central agency system in FHFA's *Supply Chain Risk Management Strategy* were still ongoing. An FHFA official stated that FHFA will create a document repository in its agency-wide document management system to store self-attestation letters.

FHFA officials were also aware of forthcoming rules from the Federal Acquisition Regulatory (FAR) Council¹⁸ that could affect the *Supply Chain Risk Management Strategy* document updates, contributing to the delays. An OTIM official stated that since the FAR updates have not been finalized, FHFA could not develop training in accordance with OMB M-22-18. In addition, the same OTIM official stated that once the FAR requirements are finalized, any associated training requirements will be adapted to the final FAR rule changes, as applicable, and assigned to the FHFA cognizant contracting officer representatives and purchase card holders. Further, since FHFA officials were actively having these discussions to update the *Supply Chain Risk Management Strategy*, they did not consider requesting an extension or a waiver to the requirements of OMB M-22-18.

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*¹⁹ (May 12, 2021), focuses on the security and integrity of the software supply chain²⁰ and emphasizes the importance of secure software development environments. The EO directs the NIST to issue guidance "identifying practices that enhance the security of the software supply chain." The NIST SP 800-218 and the NIST's *Software Supply Chain Security Guidance* under EO 14028 Section 4e²¹ (February 4, 2022) includes a set of practices that create the foundation for developing secure software.

Consistent with EO 14028, OMB M-22-18 requires each federal agency to comply with the NIST Guidance when using third-party software on the agency's information systems or otherwise affecting the agency's information.²² The NIST Guidance provides "recommendations to federal agencies on ensuring that the producers of software they procure have been following a risk-based approach for secure software development." The OMB M-22-18 further requires agencies to develop a process to communicate these requirements to producers, and to collect attestation letters from the software producers. Federal agencies must only use software provided by software producers who can attest to complying with the Government-specified secure software development practices, as described in the NIST Guidance. Specifically, Chief Information Officers, in coordination with requiring offices and Chief Acquisition Officers, must take the following steps to ensure software producers have implemented and will attest to conformity with secure software development practices.

¹⁸ The FAR Council was established to assist in the direction and coordination of Government-wide procurement policy and Government-wide procurement regulatory activities in the Federal Government, in accordance with Title 41, Chapter 7, Section 421 of the Office of Federal Procurement Policy Act.

¹⁹ See EO 14028 online [here](#).

²⁰ In 2020, there was a significant supply chain incident in which software producer was breached, giving hackers access to government agency and private company systems using this software. Federal agencies are now being assessed on their efforts to address supply chain risk exposure. A Supply Chain Risk Management category was added to the FY2021 IG FISMA Reporting Metrics focusing on the maturity of an agency's supply chain risk management strategies, plans, policies, procedures, and processes to ensure that products, systems, system components, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements. In order to mitigate future attacks, it is imperative that processes and controls are in place to prevent and detect supply chain threats.

²¹ See NIST's Software Supply Chain Security Guidance under EO 14028 Section 4e online [here](#).

²² See OMB M-22-18 online [here](#).

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

1. Consistent with the NIST Guidance and by the timelines identified below, agencies are required to obtain a self-attestation from the software producer before using the software.
 - a) A software producer's self-attestation serves as a "conformance statement" described by the NIST Guidance. The agency must obtain a self-attestation for all third-party software subject to the requirements of this memorandum used by the agency, including software renewals and major version changes.
 - i. Agencies should encourage software producers to be product inclusive so that the same attestation may be readily provided to all purchasing agencies.
 - ii. If the software producer cannot attest to one or more practices from the NIST Guidance identified in the standard self-attestation form, the requesting agency shall require the software producer to identify those practices to which they cannot attest, document practices they have in place to mitigate those risks and require a Plan of Action & Milestones to be developed. The agency shall take appropriate steps to ensure that such documentation is not posted publicly, either by the vendor or by the agency itself. If the software producer supplies that documentation and the agency finds it satisfactory, the agency may use the software despite the producer's inability to provide a complete self-attestation.

Documentation provided in lieu of a complete self-attestation, as described in the preceding paragraph, shall not be posted publicly by the vendor or the agency.
 - b) The agency shall retain the self-attestation document unless the software producer posts it publicly and provides a link to the posting as part of its proposal response.
 - c) An acceptable self-attestation must include the following minimum requirements:
 - i. The software producer's name;
 - ii. A description of which product or products the statement refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to federal agencies);
 - iii. A statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self-attestation form; and
 - iv. Self-attestation is the minimum level required; however, agencies may make risk-based determinations that a third-party assessment is required due to the criticality of the service or product that is being acquired, as defined in OMB M-21-30.
 - d) A third-party assessment provided by either a certified Federal Risk and Authorization Management Program Third Party Assessor Organization (3PAO) or one approved by the agency shall be acceptable in lieu of a software producer's self-attestation, including in the case of open-source software or products incorporating open-source software, provided the 3PAO uses the NIST Guidance as the assessment baseline.
 - e) Agencies are encouraged to use a standard self-attestation form, which will be made available to agencies. The FAR Council plans to propose rulemaking on the use of a uniform standard self-attestation form.

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

2. Agencies may obtain from software producers artifacts that demonstrate conformance to secure software development practices, as needed.
 - a) A Software Bill of Materials (SBOMs) may be required by the agency in solicitation requirements, based on the criticality of the software as defined in OMB M-21-30, or as determined by the agency. If required, the SBOM shall be retained by the agency, unless the software producer posts it publicly and provides a link to that posting to the agency.
 - b) SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration report "*The Minimum Elements for a Software Bill of Materials*," or successor guidance as published by the Cybersecurity and Infrastructure Security Agency.
 - c) Agencies shall consider reciprocity of SBOM and other artifacts from software producers that are maintained by other federal agencies, based on direct applicability and currency of the artifacts.
 - d) Artifacts other than the SBOM (e.g., from the use of automated tools and processes which validate the integrity of the source code and check for known or potential vulnerabilities) may be required if the agency determines them necessary.
 - e) Evidence that the software producer participates in a Vulnerability Disclosure Program may be required by the agency.
 - f) Agencies are encouraged to notify potential vendors of requirements as early in the acquisition process as feasible, including leveraging pre-solicitation activities.

Further, OMB M-22-18 requires agencies to perform the following:

1. Within 90 days of the date of this memorandum [or by December 13, 2022], agencies shall inventory all software subject to the requirements of this memorandum, with a separate inventory for "critical software."
2. Within 120 days of the date of this memorandum [or by January 12, 2023], agencies shall develop a consistent process to communicate relevant requirements in this memorandum to vendors and ensure attestation letters not posted publicly by software providers are collected in one central agency system.
3. Agencies shall collect attestation letters not posted publicly by software providers for "critical software" subject to the requirements of this memorandum within 270 days after publication of this memorandum [or by June 11, 2023].²³
4. Agencies shall collect attestation letters not posted publicly by software providers for all software subject to the requirements of this memorandum within 365 days after publication of this memorandum [or by September 14, 2023].²⁴

²³ On June 9, 2023, OMB Memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, was published extending the due dates for agencies to collect attestation letters for "critical software" until 3 months after OMB Paper Reduction Act (PRA) approval of common form. Additionally, it extends the due date for agencies to collect attestation letters for all software subject to the requirements of OMB M-22-18 until 6 months after OMB PRA approval of common form.

²⁴ See footnote 23.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

5. Within 180 days of the date of this memorandum [or by March 13, 2023], agency Chief Information Officers, in coordination with agency requiring activities and agency Chief Acquisition Officers, shall assess organizational training needs and develop training plans for the review and validation of full attestation documents and artifacts.
6. *Extensions.* Agencies may request an extension for complying with the requirements of this memorandum. The extension request shall be submitted to the Director of OMB and must be transmitted 30 days before any relevant deadline in this memorandum and accompanied by a plan for meeting the underlying requirements. Specific instructions for submitting requests for extensions will be posted in MAX.gov at this URL: <https://community.max.gov/x/LhtGJw>.
7. *Waivers.* Agencies may request a waiver—only in the case of exceptional circumstances and for a limited duration—for any specific requirement(s) of this memorandum. The waiver request must be submitted to the Director of OMB and must be transmitted 30 days before any relevant deadline in this memorandum and accompanied by a plan for mitigating any potential risks. The Director of OMB, in consultation with the Assistant to the President and National Security Advisor, will consider granting the request on a case-by-case basis. Specific instructions for submitting requests for waivers will be posted in MAX at this URL: <https://community.max.gov/x/LhtGJw>.
8. *Compliance with Other Authorities.* In executing the activities required by this memorandum, agencies shall comply with laws governing the collection, use, and dissemination of information.

The lack of appropriate planning to integrate the NIST Guidance into FHFA's *Supply Chain Risk Management Strategy*, increases the risk that FHFA will not have assurances from software producers that their software is in compliance with the NIST-specified secure software development practices by the OMB required deadline. Additionally, not having self-attestation letters, associated evidence of conformance from software producers (as needed), and training to validate self-attestation letters may result in FHFA using less secure software that may expose FHFA's systems and networks to vulnerabilities and exploits by bad actors.

By not establishing a centrally located repository in FHFA's document management system to store self-attestation letters from the software producers that are not publicly available, there may be increased risk that FHFA may not effectively retain and catalog these self-attestation letters. Without requesting an extension or a waiver from OMB and documenting a plan for mitigating any potential risk for noncompliance with OMB M-22-18 requirements, FHFA missed an opportunity to perform the proper planning to become compliant.

We recommend that FHFA's Acting Chief Information Officer:

- Recommendation 1:*** *Update FHFA's Supply Chain Risk Management Strategy to include past due OMB M-22-18 requirements including:*
- i. Obtaining a self-attestation from the software producer before using the software;*
 - ii. Obtaining from software producers artifacts that demonstrate conformance to secure software development practices, as needed;*
 - iii. Establishing a system to store self-attestation letters from the software producer that are not publicly available in a central location; and*

Federal Housing Finance Agency
FY 2023 Audit of FHFA’s Information Security Programs and Practices

- iv. Assessing and developing training for reviewing and validating self-attestation letters.*

Recommendation 2: *If FHFA is unable to meet the requirements in OMB M-22-18 and/or OMB M-23-16 in a timely manner, FHFA should consider request for an extension or waiver in accordance with OMB M-22-18 and/or OMB M-23-16. If FHFA requests a waiver, FHFA should consider documenting a risk-based decision, and document any compensating controls.*

2. Weaknesses in FHFA-OIG’s Supply Chain Risk Management Controls

Cybersecurity Framework Security Function: *Identify*
FY 2023 IG FISMA Reporting Metrics Domain: *Supply Chain Risk Management*

As required by the OMB M-22-18, we found that FHFA-OIG created an inventory of “critical software”²⁵ within 90 days or by December 13, 2022.

During fieldwork testing, we noted that the *Supply Chain Risk Management Plan* document did not include OMB M-22-18 requirements within 120 days or by January 12, 2023. Specifically, FHFA-OIG’s *Supply Chain Risk Management Plan* document did not include a process to communicate relevant secure software development requirements to software producers that include the following requirements:

- (1) Obtaining from software producers a “conformance statement” (i.e., a self-attestation letter) attesting their software development processes follow secure software development practices;
- (2) Obtaining from software producers artifacts that demonstrate conformance to secure software development practices, as needed; and
- (3) Establishing a system to store self-attestation letters from software producers that are not publicly available in a central location.

We were informed by FHFA-OIG officials, that the *Supply Chain Risk Management Plan* was in draft but was not finalized at the time to cover the abovementioned requirements. After our notification in February 2023, FHFA-OIG finalized the *Supply Chain Risk Management Plan* document to include the abovementioned requirements, except for the SBOM.

Additionally, FHFA-OIG did not request from OMB an extension, or a waiver, nor document a plan for mitigating any potential risk, for not complying with any of the requirements of OMB M-22-18.

An FHFA-OIG official stated that the updated *Supply Chain Risk Management Plan* document was not finalized because FHFA-OIG understood it had met the requirement of OMB M-22-18 by a) developing a consistent process to integrate NIST guidance and requirements of OMB M-22-18 into its software evaluation process and b) by documenting this process within its updated *Supply Chain Risk Management Plan*, while awaiting additional guidance and forthcoming rules from the Federal Acquisition Regulatory Council. FHFA-OIG officials stated this process was discussed, planned, and coordinated with key stakeholders and was documented in the update to FHFA-OIG’s *Supply Chain Risk Management Plan* within 120 days of the date of the memorandum. FHFA-OIG officials stated that they did not believe that requesting an extension or a waiver, accompanied by a plan for mitigating any potential risks, was required or appropriate

²⁵ See footnote 15.

Federal Housing Finance Agency
FY 2023 Audit of FHFA’s Information Security Programs and Practices

since FHFA-OIG believes it met the requirement of OMB M-22-18 “to develop a consistent process.” An FHFA-OIG official stated, since the SBOM is currently at the discretion of the agency, the FHFA-OIG has chosen not to include this requirement at this time in its *Supply Chain Risk Management Plan*. The same FHFA-OIG official stated, if and when FHFA-OIG determines SBOMs are needed, FHFA-OIG will align their procedures with OMB M-22-18.

EO 14028²⁶ focuses on the security and integrity of the software supply chain²⁷ and emphasizes the importance of secure software development environments. The EO directs the NIST to issue guidance “identifying practices that enhance the security of the software supply chain.” The NIST SP 800-218 and the NIST’s *Software Supply Chain Security Guidance* under EO 14028 Section 4e²⁸ includes a set of practices that create the foundation for developing secure software.

Consistent with EO 14028, OMB M-22-18 requires each federal agency to comply with the NIST Guidance when using third-party software on the agency’s information systems or otherwise affecting the agency’s information.²⁹ The NIST Guidance provides “recommendations to federal agencies on ensuring that the producers of software they procure have been following a risk-based approach for secure software development.” The OMB M-22-18 further requires agencies to develop a process to communicate these requirements to producers, and to collect attestation letters from the software producers. Federal agencies must only use software provided by software producers who can attest to complying with the Government-specified secure software development practices, as described in the NIST Guidance. Specifically, Chief Information Officers, in coordination with requiring offices and Chief Acquisition Officers, must take the following steps to ensure software producers have implemented and will attest to conformity with secure software development practices:

1. Consistent with the NIST Guidance and by the timelines identified below, agencies are required to obtain a self-attestation from the software producer before using the software.
 - a) A software producer’s self-attestation serves as a “conformance statement” described by the NIST Guidance. The agency must obtain a self-attestation for all third-party software subject to the requirements of this memorandum used by the agency, including software renewals and major version changes:
 - i. Agencies should encourage software producers to be product inclusive so that the same attestation may be readily provided to all purchasing agencies.
 - ii. If the software producer cannot attest to one or more practices from the NIST Guidance identified in the standard self-attestation form, the requesting agency shall require the software producer to identify those practices to which they cannot attest, document practices they have in place to mitigate those risks and require a Plan of Action & Milestones to be developed. The agency shall take appropriate steps to ensure that such documentation is not posted publicly, either by the vendor or by the agency itself. If the software producer supplies that documentation and the agency finds it satisfactory, the agency may use the software despite the producer’s inability to provide a complete self-attestation.

²⁶ See footnote 19.

²⁷ See footnote 20.

²⁸ See footnote 21.

²⁹ See footnote 22.

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

Documentation provided in lieu of a complete self-attestation, as described in the preceding paragraph, shall not be posted publicly by the vendor or the agency.

- b) The agency shall retain the self-attestation document unless the software producer posts it publicly and provides a link to the posting as part of its proposal response.
 - c) An acceptable self-attestation must include the following minimum requirements:
 - i. The software producer's name;
 - ii. A description of which product or products the statement refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to federal agencies);
 - iii. A statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self-attestation form; and
 - iv. Self-attestation is the minimum level required; however, agencies may make risk-based determinations that a third-party assessment is required due to the criticality of the service or product that is being acquired, as defined in OMB M-21-30.
 - d) A third-party assessment provided by either a certified Federal Risk and Authorization Management Program 3PAO or one approved by the agency shall be acceptable in lieu of a software producer's self-attestation, including in the case of open-source software or products incorporating open-source software, provided the 3PAO uses the NIST Guidance as the assessment baseline.
 - e) Agencies are encouraged to use a standard self-attestation form, which will be made available to agencies. The FAR Council plans to propose rulemaking on the use of a uniform standard self-attestation form.
2. Agencies may obtain from software producers artifacts that demonstrate conformance to secure software development practices, as needed.
- a) SBOMs may be required by the agency in solicitation requirements, based on the criticality of the software as defined in OMB M-21-30, or as determined by the agency. If required, the SBOM shall be retained by the agency, unless the software producer posts it publicly and provides a link to that posting to the agency.
 - b) SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration report "*The Minimum Elements for a Software Bill of Materials (SBOM)*," or successor guidance as published by the Cybersecurity and Infrastructure Security Agency.
 - c) Agencies shall consider reciprocity of SBOM and other artifacts from software producers that are maintained by other federal agencies, based on direct applicability and currency of the artifacts.
 - d) Artifacts other than the SBOM (e.g., from the use of automated tools and processes which validate the integrity of the source code and check for known or potential vulnerabilities) may be required if the agency determines them necessary.
 - e) Evidence that the software producer participates in a Vulnerability Disclosure Program may be required by the agency.

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

- f) Agencies are encouraged to notify potential vendors of requirements as early in the acquisition process as feasible, including leveraging pre-solicitation activities.

Further, OMB M-22-18 requires agencies to perform the following:

1. Within 90 days of the date of this memorandum [or by December 13, 2022], agencies shall inventory all software subject to the requirements of this memorandum, with a separate inventory for “critical software.”
2. Within 120 days of the date of this memorandum [or by January 12, 2023], agencies shall develop a consistent process to communicate relevant requirements in this memorandum to vendors and ensure attestation letters not posted publicly by software providers are collected in one central agency system.
3. Agencies shall collect attestation letters not posted publicly by software providers for “critical software” subject to the requirements of this memorandum within 270 days after publication of this memorandum [or by June 11, 2023].³⁰
4. Agencies shall collect attestation letters not posted publicly by software providers for all software subject to the requirements of this memorandum within 365 days after publication of this memorandum [or by September 14, 2023].³¹
5. Within 180 days of the date of this memorandum [or by March 13, 2023], agency Chief Information Officers, in coordination with agency requiring activities and agency Chief Acquisition Officers, shall assess organizational training needs and develop training plans for the review and validation of full attestation documents and artifacts.
6. *Extensions.* Agencies may request an extension for complying with the requirements of this memorandum. The extension request shall be submitted to the Director of OMB and must be transmitted 30 days before any relevant deadline in this memorandum and accompanied by a plan for meeting the underlying requirements. Specific instructions for submitting requests for extensions will be posted in MAX.gov at this URL: <https://community.max.gov/x/LhtGJw>.
7. *Waivers.* Agencies may request a waiver—only in the case of exceptional circumstances and for a limited duration—for any specific requirement(s) of this memorandum. The waiver request must be submitted to the Director of OMB and must be transmitted 30 days before any relevant deadline in this memorandum and accompanied by a plan for mitigating any potential risks. The Director of OMB, in consultation with the Assistant to the President and National Security Advisor, will consider granting the request on a case-by-case basis. Specific instructions for submitting requests for waivers will be posted in MAX at this URL: <https://community.max.gov/x/LhtGJw>.
8. *Compliance with Other Authorities.* In executing the activities required by this memorandum, agencies shall comply with laws governing the collection, use, and dissemination of information.

Without finalizing a process to communicate relevant requirements, as documented in OMB M-22-18, the risk that FHFA-OIG will not be able to collect assurances from software producers that

³⁰ See footnote 23.

³¹ See footnote 23.

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

their software is in compliance with the NIST specified secure software development practices by the OMB required deadline may be increased.

By not establishing a system to store self-attestation letters from the software producers that are not publicly available in a central location, the risk that FHFA-OIG may not properly retain and catalog these self-attestation letters may be increased. In addition, by not requesting an extension or a waiver from OMB or documenting a plan for mitigating any potential risk for not complying with OMB M-22-18 requirements prior to January 12, 2023, FHFA-OIG missed an opportunity to take the time to perform the proper planning to be in compliance with OMB M-22-18 requirements.

Upon notification, FHFA-OIG took action by finalizing its *Supply Chain Risk Management Plan* to include requirements around: requesting and obtaining self-attestation letters; evaluating software by going through the FHFA-OIG information technology process before a new contract can start; and identifying a storage location for self-attestation letters. Therefore, we made no recommendation related to this plan.

3. Weaknesses in FHFA's Vulnerability Management

Cybersecurity Framework Security Function: *Protect*

FY 2023 IG FISMA Reporting Metrics Domain: *Configuration Management*

Based on our analysis of the Qualys³² Asset Vulnerability Report (April 7, 2023), we found that of FHFA's 2,820 reported vulnerabilities, OTIM did not remediate 1,716 Cybersecurity and Infrastructure Security Agency (CISA) Known Exploitable Vulnerabilities within 14 days of first discovery in accordance with CISA and OITM requirements. The discovery of past due vulnerabilities ranged between August 10, 2022, to March 24, 2023.

In addition, FHFA did not create plan of actions and milestones (POA&Ms)³³ for remediating these security weaknesses.

OTIM officials stated that for most of the identified vulnerabilities, FHFA's attempts to remediate these vulnerabilities failed. After extensive troubleshooting, OTIM officials stated they will create POA&Ms to remediate the vulnerabilities. In addition, we were not informed of any additional risk mitigation strategies (i.e., system isolation) that FHFA plans to deploy, in the meantime, to mitigate the risk related to the vulnerable systems.

CISA's Binding Operating Directive (BOD)³⁴ 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, requires that CISA known exploitable vulnerabilities are remediated within 14 days. CISA has established a catalog of known exploited vulnerabilities that carry significant risk to the federal agencies and establishes requirements for agencies to remediate such vulnerabilities.³⁵

³² Qualys is utilized by FHFA as its vulnerability scanning solution. Qualys is a risk-based vulnerability management solution utilized to prioritize vulnerabilities and assets based on risk.

³³ 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.

³⁴ CISA, an operational component under Department of Homeland Security, develops and oversees the implementation of BODs, which require action on the part of certain federal agencies in the civilian Executive Branch. These directives require agencies to complete required actions to protect federal information and information systems from known information security threats, vulnerabilities, and risks.

³⁵ See CISA's known exploitable vulnerabilities online [here](#).

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

Consistent with CISA requirements, the *OTIM Vulnerability Management Process*, Revision 2.7 (September 7, 2022), has established target remediation timeframes based on the vulnerability severity rating. Further, the process requires that CISA known exploitable vulnerabilities are remediated within 14 days.

NIST 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.

Hackers could exploit vulnerabilities to take control of systems to cause a denial-of-service attack,³⁶ or to allow unauthorized access and malicious modification to FHFA's systems and data. Vulnerabilities that remain un-remediated over an extended period of time increase exposure and likelihood that the confidentiality, integrity, and availability of FHFA systems and data can be compromised.

We recommend that FHFA's Acting Chief Information Officer:

Recommendation 3: Remediate past due exploitable vulnerabilities in accordance with CISA's BOD 22-01 and the OTIM Vulnerability Management Process.

Recommendation 4: Develop POA&Ms to track the remediation of past due CISA known exploitable vulnerabilities that cannot be remediated in a timely manner (within 14 days) in accordance with CISA's BOD 22-01 and OTIM Vulnerability Management Process. Consider implementing compensating controls (i.e., isolating systems with un-remediated vulnerabilities) to mitigate the risk of the vulnerabilities.

4. Weaknesses in FHFA's Event Logging Maturity

Cybersecurity Framework Security Function: Respond
FY 2023 IG FISMA Reporting Metrics Domain: Incident Response

Based on our review of FHFA's *M-21-31 Project Plan* received on March 2, 2023, we determined that FHFA Event Logging (EL) maturity level is at EL0,³⁷ which is not-effective. FHFA also assessed its EL maturity against the requirements in OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021), and reported the maturity level as EL0, not-effective. While FHFA has documented a detailed *Project Plan* to assist with reaching compliance with OMB M-21-31 requirements, FHFA did not reach EL1³⁸ and EL2³⁹ maturity levels by OMB's required due dates. Specifically, FHFA did not meet the following:

- within one year of the date of OMB M-21-31, or by August 27, 2022, reach EL1 maturity level; and
- within 18 months of the date of OMB M-21-31, or by February 27, 2023, achieve EL2 maturity level.

³⁶ A denial-of-service attack is an attack meant to shut down a system or network making it inaccessible to its intended users.

³⁷ Per OMB M-21-31, EL0 maturity level signifies logging requirements of highest criticality are either not met or are only partially met.

³⁸ Per OMB M-21-31, EL1 maturity level signifies only logging requirements of highest criticality are met.

³⁹ Per OMB M-21-31, EL2 maturity level signifies logging requirements of highest and intermediate criticality are met.

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

Further, FHFA did not document any risk-based decisions, including compensating controls, for not meeting the requirements in OMB M-21-31.

OTIM officials stated that OTIM was researching what actions can be implemented for systems that do not natively⁴⁰ forward event logs to the Security Information and Event Management (SIEM)⁴¹ tool. In addition, this research took time and resources and was a leading factor in not meeting EL1 and EL2 maturity levels by the required deadlines. At the time, FHFA was actively researching solutions, and did not consider documenting risk acceptances related to OMB M-21-31. OTIM officials have stated that FHFA will consider documenting risk acceptances for those systems where a solution to forward event logs to the SIEM does not exist and the level of effort is determined to be not cost effective or appropriate.

OMB M-21-31 addresses the logging requirements in the EO 14028.⁴² OMB M-21-31 establishes a maturity model to guide the implementation of requirements across EL tiers as shown below that are designed to help agencies prioritize their efforts and resources to achieve full compliance with requirements for implementation, log categories, and centralized access. OMB M-21-31 further requires that agencies forward all required event logs, in near real-time and on an automated basis, to centralized systems responsible for SIEM.

The maturity model to guide the implementation of requirements is summarized below:

Tier EL0, Rating – Not Effective

The agency or one or more of its components have not implemented the following requirement:

- Ensuring that the Required Logs categorized as Criticality Level 0 are retained in acceptable formats for specified timeframes, per technical details described in OMB M-21-31, Appendix C (Logging Requirements – Technical Details).

Tier EL1, Rating – Basic (to be met by August 27, 2022)

The agency and all of its components meet the following requirements, as detailed in Table 2 (EL1 Basic Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Basic Logging Categories
- Minimum Logging Data
- Time Standard
- Event Forwarding
- Protecting and Validating Log Information
- Passive DNS [Domain Name System]
- CISA and Federal Bureau of Investigations Access Requirements

⁴⁰ System audit logs are not in a format that can be accepted by the SIEM tool.

⁴¹ SIEM tools are a type of centralized logging software that can facilitate the aggregation and consolidation of audit log records from multiple information system components. SIEM tools automate the collection of audit log records from tools and report them to a management console in a standardized format. SIEM tools facilitate audit record correlation and analysis. The correlation of audit log record information with all components of an organization's network and business applications provides additional tools that may assist in determining the veracity and scope of potential attacks. SIEM products usually include support for many types of audit log record sources, such as operating systems, applications, and security software. A SIEM server analyzes the data from all the different audit log record sources, correlates events among the audit log record entries, identifies and prioritizes significant events, and can be configured to initiate responses to events.

⁴² See footnote 19.

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

- Logging Orchestration, Automation, and Response – Planning
- User Behavior Monitoring – Planning
- Basic Centralized Access

Tier EL2, Rating – Intermediate (to be met by February 26, 2023)

The agency and all of its components meet the following requirements, as detailed in Table 3 (EL2 Intermediate Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Meeting EL1 maturity level
- Intermediate Logging Categories
- Publication of Standardized Log Structure
- Inspection of Encrypted Data
- Intermediate Centralized Access

Tier EL3, Rating – Advanced (to be met by August 27, 2023)

The agency and all its components meet the following requirements, as detailed in in Table 4 (EL3 Advanced Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Meeting EL2 maturity level
- Advanced Logging Categories
- Logging Orchestration, Automation, and Response – Finalizing Implementation
- User Behavior Monitoring – Finalizing Implementation
- Application Container Security, Operations, and Management
- Advanced Centralized Access

Further, OMB M-21-31, Section II: Agency Implementation Requirements, requires agencies to perform the following:

- Within 60 calendar days of the date of OMB M-21-31 [or by October 26, 2021] memorandum, assess their maturity against the maturity model in OMB M-21-31 and identify resourcing and implementation gaps associated with completing each of the requirements listed below. Agencies will provide their plans and estimates to their OMB Resource Management Office and Office of the Federal Chief Information Officer desk officer.
- Within one year of the date of OMB Memorandum 21-31 [or by August 27, 2022], reach EL1 maturity.
- Within 18 months of OMB M-21-31 [or by February 26, 2023], achieve EL2 maturity.
- Within two years of OMB Memorandum 21-31 [or by August 27, 2023], achieve EL3 maturity.
- Provide, upon request and to the extent consistent with applicable law, relevant logs to the CISA and Federal Bureau of Investigations. This sharing of information is critical to defend federal information systems.
- Share log information, as needed and appropriate, with other federal agencies to address cybersecurity risks or incidents.

Cyber-attacks underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud services providers) is invaluable in the detection, investigation, and remediation of cyber threats. By not achieving EL1

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

and EL2 maturity levels, FHFA is not meeting logging requirements of highest criticality. FHFA maturity is currently at EL0 maturity; therefore, its event logging capabilities are not effective based on OMB M-21-31. Further, FHFA may not correlate audit log records across different repositories in a complete or risk-based manner, which may increase the risk that FHFA may not collect all meaningful and relevant data on suspicious events. This may, in turn increase the risk that FHFA may inadvertently miss the potential scope or veracity of suspicious events or attacks.

We recommend that FHFA's Acting Chief Information Officer:

Recommendation 5: *Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.*

Recommendation 6: *Identify and implement solutions, in coordination with vendors, where a solution does not exist for systems to natively forward event logs to the SIEM tool. If there are no viable solutions, perform a risk assessment and cost benefit analysis. Based on the risk assessment, document any risk-based decisions, including compensating controls, for systems not in compliance with OMB M-21-31.*

5. Weaknesses in FHFA-OIG's Event Logging Maturity

Cybersecurity Framework Security Function: *Respond*
FY 2023 IG FISMA Reporting Metrics Domain: *Incident Response*

Based on a review of FHFA-OIG's *OMB M-21-31 Agency Component Tracker* received on March 2, 2023, we determined that FHFA-OIG's EL maturity level is at EL0,⁴³ which is not-effective. FHFA-OIG also assessed its EL maturity against the requirements in OMB M-21-31 and reported the maturity level as EL0, not-effective. While FHFA-OIG has documented an *Agency Component Tracker* to assist with reaching compliance with OMB M-21-31 requirements, FHFA-OIG did not reach EL1⁴⁴ and EL2⁴⁵ maturity levels. Specifically, FHFA-OIG did not meet the following:

- within one year of the date of OMB M-21-31, or by August 27, 2022, achieve EL1 maturity.
- within 18 months of the date of OMB M-21-31, or by February 27, 2023, achieve EL2 maturity.

FHFA-OIG opened a POA&M⁴⁶ in September 2022 related to specific actions required to meet EL1 and EL2 maturity. Within this POA&M, there was a tentative milestone to document any risk acceptances for solutions that may not be feasible. However, this tentative milestone was delayed due to additional engineering and vendor support required to research solutions.

An FHFA-OIG official stated that FHFA-OIG did not reach EL1 and EL2 maturity levels because it had some unencrypted audit log records forwarded from internal systems to its SIEM tool. This led to additional engineering and vendor support to research solutions and a delay in meeting the requirements.

OMB M-21-31 addresses the logging requirements in the EO 14028 and establishes a maturity model to guide the implementation of requirements across EL tiers as shown below that are

⁴³ See footnote 38.

⁴⁴ See footnote 39.

⁴⁵ See footnote 40.

⁴⁶ See footnote 34.

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

designed to help agencies prioritize their efforts and resources to achieve full compliance with requirements for implementation, log categories, and centralized access. OMB M-21-31 further requires that agencies forward all required event logs, in near real-time and on an automated basis, to centralized systems responsible for SIEM.

The maturity model to guide the implementation of requirements is summarized below:

Tier EL0, Rating – Not Effective

The agency or one or more of its components have not implemented the following requirement:

- Ensuring that the Required Logs categorized as Criticality Level 0 are retained in acceptable formats for specified timeframes, per technical details described in OMB M-21-31, Appendix C (Logging Requirements – Technical Details).

Tier EL1, Rating – Basic (to be met by August 27, 2022)

The agency and all of its components meet the following requirements, as detailed in Table 2 (EL1 Basic Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Basic Logging Categories
- Minimum Logging Data
- Time Standard
- Event Forwarding
- Protecting and Validating Log Information
- Passive DNS
- CISA and Federal Bureau of Investigations Access Requirements
- Logging Orchestration, Automation, and Response – Planning
- User Behavior Monitoring – Planning
- Basic Centralized Access

Tier EL2, Rating – Intermediate (to be met by February 26, 2023)

The agency and all of its components meet the following requirements, as detailed in Table 3 (EL2 Intermediate Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Meeting EL1 maturity level
- Intermediate Logging Categories
- Publication of Standardized Log Structure
- Inspection of Encrypted Data
- Intermediate Centralized Access

Tier EL3, Rating – Advanced (to be met by August 27, 2023)

The agency and all its components meet the following requirements, as detailed in in Table 4 (EL3 Advanced Requirements) within OMB M-21-31, Appendix A (Implementation and Centralized Access Requirements):

- Meeting EL2 maturity level
- Advanced Logging Categories
- Logging Orchestration, Automation, and Response – Finalizing Implementation

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

- User Behavior Monitoring – Finalizing Implementation
- Application Container Security, Operations, and Management
- Advanced Centralized Access

Further, OMB M-21-31, Section II: Agency Implementation Requirements, requires agencies to perform the following:

- Within 60 calendar days of the date of OMB M-21-31 [or by October 26, 2021] memorandum, assess their maturity against the maturity model in OMB M-21-31 and identify resourcing and implementation gaps associated with completing each of the requirements listed below. Agencies will provide their plans and estimates to their OMB Resource Management Office and Office of the Federal Chief Information Officer desk officer.
- Within one year of the date of OMB M-21-31 [or by August 27, 2022], reach EL1 maturity.
- Within 18 months of OMB M-21-31 [or by February 26, 2023], achieve EL2 maturity.
- Within two years of OMB M-21-31 [or by August 27, 2023], achieve EL3 maturity.
- Provide, upon request and to the extent consistent with applicable law, relevant logs to the CISA and Federal Bureau of Investigations. This sharing of information is critical to defend federal information systems.
- Share log information, as needed and appropriate, with other federal agencies to address cybersecurity risks or incidents.

Cyber-attacks underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud services providers) is invaluable in the detection, investigation, and remediation of cyber threats. FHFA-OIG's maturity is currently at EL0 maturity, as the requirements for EL1 were partially met; therefore, their event logging capabilities are not effective based on OMB M-21-31. This may increase the risk that unencrypted sensitive internal log information may be intercepted.

We recommend that FHFA-OIG's Chief Information Officer perform the following corrective actions in accordance with the existing, related POA&M:

Recommendation 7: Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.

Recommendation 8: Identify and implement solutions, in coordination with vendors and engineering team, to encrypt logs in transit between the source system and SIEM tool. If there are no viable solutions, perform a risk assessment and cost benefit analysis. Based the risk assessment, document any risk-based decisions, including compensating controls, for systems not in compliance with OMB M-21-31.

6. Weaknesses in FHFA's Incident Response Plans and Procedures

Cybersecurity Framework Security Function: *Respond*
FY 2023 IG FISMA Reporting Metrics Domain: *Incident Response*

We found that FHFA did not update all incident response plans and procedures to reflect the three-year review cycle outlined in its *Incident Response Standard* (November 30, 2022), version 2.1. Specifically, we noted the following plans and procedures were not updated:

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

- *Cyber Incident Reporting Procedures*, Revision 1.0 (December 7, 2021);
- *FHFA Information Incident and Breach Response Plan*, Revision 5.0 (September 1, 2021). Upon notification in February 2023, OTIM took corrective action and completed the review and approval of the *FHFA Information Incident and Breach Response Plan*, Revision 5.2, as of March 30, 2023; and
- *FHFA Common Control Plan* (July 16, 2021).

OTIM officials stated that their IT policies, procedures, and standards were relatively stable, and that changes to them on an annual basis were typically minor, as such, management made a decision to revise the frequency of their reviews to every three-years or as necessary. OTIM had started updating the frequency of review within various IT policies, procedures, and standards documents. However, OTIM did not update the newly defined frequency for reviews of incident response plans and procedures in the *Cyber Incident Reporting Procedures*, the *FHFA Information Incident and Breach Response Plan*, and the *FHFA Common Control Plan*; thus, creating inconsistent frequency of review statements. The OTIM official stated that OTIM had plans to review these documents during the new three-year review cycle.

NIST SP 800-53, Revision 5, security control Incident Response (IR)-1, required that agencies review and update the current incident response policy and procedures following organizationally defined frequency or organizationally defined events.

FHFA's *Incident Response Standard*, Revision 2.1 (November 30, 2022), states that:

OTIM reviews all IT policies, procedures and standards and updates them, as necessary, but at least every three-years, to ensure they are still applicable to the FHFA environment, and compliant with applicable federal laws, directives, policies, regulations, standards, and guidance.

By not updating all of its incident response plans, policies, and procedures to reflect the three-year review cycle as required, FHFA risks that its incident response plan, policies, and procedures may result in inconsistencies. Furthermore, this may increase the risk of incident response process documentation may not be compliant with applicable federal laws, directives, policies, regulations, standards, and guidance.

Upon notification, FHFA took action to correct the weakness related to the *FHFA Information Incident and Breach Response Plan*; therefore, we made no recommendation related to this plan. However, we made recommendations related to the other two incident response plans and procedures.

We recommend that FHFA's Acting Chief Information Officer:

Recommendation 9: *Review and update the Cyber Incident Reporting Procedures, and the FHFA Common Control Plan to ensure they include FHFA's three-year review cycle outlined in the Incident Response Standard.*

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

7. Weaknesses in FHFA's Contingency Plan Testing

Cybersecurity Framework Security Function: *Recover*

FY 2023 IG FISMA Reporting Metrics Domain: *Contingency Planning*

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

- Job Performance Plan (JPP) – The *Disaster Recovery Procedures for FHFA Production Systems* (November 9, 2022) did not make any reference to JPP's Structured Query Language (SQL)⁴⁷ server, and the annual disaster recovery exercise⁴⁸ did not include JPP's SQL server; and
- Correspondence Tracking System (CTS) – In a recent OIG Audit Report,⁴⁹ FHFA-OIG noted that FHFA's General Support System (GSS) contingency plan⁵⁰ did not reference CTS or its servers. When OTIM performed the annual GSS contingency plan testing, it did not include CTS or its servers. During our testing, we reaffirmed that OTIM did not document the recovery procedures for the SQL servers associated with CTS. We also reaffirmed that when OTIM performed the annual contingency plan testing, it did not include CTS's SQL servers.

OTIM officials stated that JPP and CTS reside on shared internal web servers and SQL servers, and the recovery procedures for these applications are documented in the *Disaster Recovery Procedures for FHFA Production Systems*. However, we found no reference to the JPP or CTS SQL servers documented in the *Disaster Recovery Procedures for FHFA Production Systems*. OTIM officials cited a lack of resources for the above shortcomings related to contingency testing. Specifically, management of the SQL servers was being transitioned to new team members, and therefore, OTIM did not have the resources to perform the JPP and CTS SQL server contingency tests at that time. OTIM officials stated that once the database responsibilities are transitioned, the new team should have the resources to participate in the next disaster recovery exercise, tentatively scheduled for late 2023.

NIST SP 800-53, Revision 5 provides a catalog of security and privacy controls, including controls specifically related to contingency planning. Taken together, for contingency planning, NIST requires organizations to:

- Establish a contingency planning policy and procedure.
- Develop and periodically update the contingency plan for each information system.
- Provide contingency training for individuals consistent with their roles and responsibilities.
- Test the contingency plan on a defined frequency.

⁴⁷ Structured Query Language, abbreviated as SQL, is a programming language designed for storing and processing information in a relational database. For example, relational databases can be thought of as a collection of spreadsheet files that help businesses organize, manage, and relate data. In the relational database model, each "spreadsheet" is a table that stores information, represented as columns (attributes) and rows (records).

⁴⁸ The *Annual Disaster Recovery Exercise* memorandum (January 5, 2023) states that the purpose of the yearly disaster recovery exercise is to validate the proper operation and resiliency and recovery measures incorporated into the overall IT infrastructure, including systems hosted on that infrastructure. FHFA's 2022 Disaster Recovery Exercise was performed in two parts on December 18, 2022, and December 22, 2022.

⁴⁹ See footnote 2.

⁵⁰ The GSS contingency plan was the previous version of the *Disaster Recovery Procedures for FHFA Production Systems* (November 9, 2022).

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (November 11, 2011), Section 3.5.1, states that:

Information System Contingency Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing can take on several forms and accomplish several objectives but should be conducted in as close to an operating environment as possible. Each information system component should be tested to confirm the accuracy of individual recovery procedures.

Consistent with NIST requirements, FHFA's *Contingency Planning Standard*, Revision 2.1 (November 30, 2022), defines the security requirements that FHFA information systems must have in support of contingency planning capabilities. The standard calls for FHFA to:

- review and update contingency plans at least annually, or at any time in which a change to the operating environment or significant change to recovery procedures has occurred; and
- test the contingency plans at least annually to determine the effectiveness of the plans and the organization readiness to execute the plans.

The lack of an annual review and testing of the JPP and CTS contingency plan increases the risk that OTIM may not recover the system successfully or timely during a disruption.

We make one new recommendation that FHFA's Acting Chief Information Officer:

Recommendation 10: Update the Disaster Recovery Procedures for FHFA Production Systems to include JPP and its servers, and ensure they are included in the annual contingency testing.

Additionally, we reaffirm two recommendations from a prior year OIG report⁵¹ that FHFA's Acting Chief Information Officer:

AUD 2022-003, Recommendation 2: Update the GSS contingency plan to include CTS and its servers and ensure CTS and its servers are included in the annual GSS contingency plan testing.

AUD 2022-003, Recommendation 3: Assess whether OTIM has sufficient, qualified staff to complete required updates and testing of its contingency plans in accordance with FHFA's standard and NIST requirements and address any resource constraints that have adversely affected OTIM's ability to carry out its contingency planning requirements.

⁵¹ See footnote 2.

EVALUATION OF MANAGERMENTS' COMMENTS

In response to a draft of this report, FHFA and FHFA-OIG provided separate management responses related to their specific program's findings and recommendations. FHFA and FHFA-OIG management agreed with all 10 recommendations in this report and outlined their plans to address each recommendation. Appendix IV includes the Agency's comments.

FHFA Response:

For recommendations 1 and 2, FHFA management agreed with these recommendations. FHFA management stated that it will perform the following actions: update its *Supply Chain Risk Management Strategy* per OMB requirements; obtain self-attestation letters from software producers; obtain artifacts that demonstrate conformance to secure software development practices, as needed; establish a dedicated centrally located network folder to store self-attestation letters from the software producers that are not publicly available; assess the need to develop training for reviewing and validating self-attestation letters; and follow OMB guidance for attestations, as it relates to non-compliant software. FHFA expects these actions to be completed by June 30, 2024. FHFA's planned corrective actions meet the intent of our recommendations.

For recommendations 3 and 4, FHFA management agreed with these recommendations. FHFA management stated that it plans to develop POA&MS to track the remediation of past-due exploitable vulnerabilities known by the CISA that cannot be remediated in a timely manner. FHFA expects these actions to be completed by September 30, 2023. FHFA's planned corrective actions meet the intent of our recommendations.

For recommendations 5 and 6, FHFA management agreed with these recommendations. FHFA management stated that it will perform the following actions: conduct a gap analysis to identify the outstanding requirements and draft a risk acceptance memo for OMB M-21-31 areas that cannot be addressed; increase storage capacity to log additional applicable sources and logging categories for all EL maturity tiers; implement logging capabilities to ensure applicable OMB M-21-31 events are logged and tracked; research Security Orchestration, Automation, and Response (SOAR) and User Behavior Monitoring solutions and assess associated costs and resource impacts to FHFA; and implement the strategies and tools to satisfy the OMB M-21-31 requirements. FHFA expects these actions to be completed by June 30, 2024. FHFA's planned corrective actions meet the intent of our recommendations.

For recommendation 9, FHFA management agreed with the recommendation. FHFA management stated that it will update the *Cyber Incident Reporting Procedures* and the *FHFA Common Control Plan* to ensure they include FHFA's three-year review cycle outlined in the *Incident Response Standard*. FHFA expects these actions to be completed by September 30, 2023. FHFA's planned corrective actions meet the intent of our recommendation.

For recommendation 10, FHFA management agreed with the recommendation. FHFA management stated that it will update its *Disaster Recovery Procedures for FHFA Production Systems* to include the servers supporting the CTS and the JPP systems and ensure they are included in the annual contingency testing. FHFA expects these actions to be completed by January 31, 2024. FHFA's planned corrective actions meet the intent of our recommendation.

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

FHFA-OIG Response:

For recommendations 7 and 8, FHFA-OIG management agreed with these recommendations. As part of the existing POA&M, FHFA-OIG previously initiated actions that address these recommendations. FHFA-OIG expects these actions to be completed by August 27, 2023. FHFA-OIG's planned corrective actions meet the intent of our recommendations.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

BACKGROUND

Federal Information Security Modernization Act of 2014

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

The statute also provides a mechanism for improved oversight of federal agency information security programs. FISMA requires agency heads⁵² 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 the 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.

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

⁵² 44 USC § 3554, Federal agency responsibilities.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

FISMA Reporting Requirements

OMB and Department of Homeland Security (DHS) annually provide instructions to federal agencies and IGs for preparing FISMA reports. On December 2, 2022, OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*.⁵³ 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 20 Supplemental IG FISMA Reporting Metrics that must be evaluated during FY 2023, in addition to the 20 Core IG FISMA Reporting Metrics that must be evaluated annually.
- The remainder of standards and controls will be evaluated on a two-year cycle.
- In previous years, IGs have been directed to utilize a mode-based scoring approach to assess maturity levels. In FY 2023, ratings were focused on calculated averages, wherein the average of the metrics in a particular domain would be used by IGs to determine the effectiveness of individual function areas (Identity, Protect, Detect, Respond, and Recover). IGs were encouraged to focus on the calculated averages of the 20 Core IG FISMA Reporting Metrics, as these tie directly to the Administration's priorities and other high-risk areas. In addition, OMB M-23-03 indicated that IGs should use the calculated averages of the Supplemental IG FISMA Reporting Metrics and progress addressing outstanding prior year recommendations as data points to support their risk-based determination of overall program and function level effectiveness. The calculated averages can be found in the FY 2023 IG FISMA Reporting Metrics, which was provided to the Agency separate from this report.

The FY 2023 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, IGs were to assess the 20 Core IG FISMA Reporting Metrics and 20 Supplemental IG FISMA Reporting Metrics in the five security function areas to assess the maturity level and effectiveness of their agency's information security program. As highlighted in **Table 3**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover.

⁵³ See OMB M-23-03 online [here](#).

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2023 IG FISMA Reporting Metrics

| Cybersecurity Framework Security Functions | Domains in the FY 2023 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 IG FISMA Reporting Metrics focus on the development of sound, risk-based policies, and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 4** below explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of Level 4, Managed and Measurable.

Table 4: IG Evaluation Maturity Levels

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

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

OBJECTIVE, SCOPE, AND METHODOLOGY

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

Objective

The objectives of this performance audit were to (1) evaluate the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines; and (2) respond to the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2023 IG FISMA Reporting Metrics).⁵⁴

Scope

The scope of this performance audit covered the Agency's information security programs and practices from April 1, 2022, through March 31, 2023. Within this period, we assessed the Agency's information security program and practices consistency with FISMA, and reporting instructions issued by OMB and DHS for FY 2023. The scope period also included assessing selected security controls from NIST SP 800-53, Revision 5, mapped to the FY 2023 IG FISMA Reporting Metrics for a sample of four systems from the 37 systems in FHFA's FISMA inventory of information systems and one system from the total population of 20 FHFA-OIG FISMA information systems (**Table 5**).

Table 5: Description of Systems Selected for Testing

| Entity | System | Description |
|----------|-------------------------------------|--|
| FHFA | CTS | CTS captures and tracks FHFA's correspondence from external sources (the public, Congress, regulated entities, etc.). |
| FHFA | Equal Employment Opportunity system | Equal Employment Opportunity complaint management gives case workers and managers the tools to guide, provide input, and report on all data elements and processes throughout ongoing and closed civil rights cases. |
| FHFA | GSS | FHFA GSS is considered a Wide Area Network and consists of the backbone, a Metropolitan Area Network and the Local Area Networks at various sites. The GSS provides connectivity between the agency's sites, Headquarters, and Datacenters; Internet access; and e-mail and directory services for all agency divisions and offices. |
| FHFA | JPP | System for managing merit pay increases and performance reviews. |
| 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 to FHFA-OIG network and central servers that support FHFA-OIG. The core network infrastructure consists of network switches, firewalls, and routers that provide boundary protection and network segmentation. |

⁵⁴ See footnote 3.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

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

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

We utilized the FY 2023 IG FISMA Reporting Metrics guidance⁵⁵ to form our conclusions for each Cybersecurity Framework domain, function, and the overall agency rating. Specifically, we focused on the calculated average of the Core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average of the Supplemental IG FISMA Reporting Metrics and progress made addressing outstanding prior year recommendations, to form our risk-based conclusion.

The audit also included an evaluation of whether FHFA took corrective action to address open recommendations from the FY 2020 FISMA audit, FY 2021 FISMA audit, FY 2021 Privacy audit, and the FY 2022 FISMA Audit.^{56,57}

Additionally, CLA leveraged the following related FHFA-OIG audit reports:

- FHFA-OIG Audit Report, AUD-2022-003, *FHFA Did Not Follow All of its Contingency Planning Requirements for the National Mortgage Database (NMDDB) or its Correspondence Tracking System (CTS)*, issued December 13, 2021.
- FHFA-OIG Audit Report, 2023-002, *FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines*, issued March 8, 2023.
- FHFA-OIG Compliance Review, COM-2023-003, *FHFA Secured Electronic Media It Designated for Disposal, But Did Not Inventory Items Consistently or Reconcile Inventory Discrepancies*, issued February 2, 2023.

⁵⁵ The FY 2023 IG FISMA Reporting Metrics provided the agency IG the discretion to determine the rating for each of the Cybersecurity Framework domains and functions and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FISMA audit. Using this approach, IGs may determine that a particular domain, function area, or agency's information security program is effective at a calculated maturity lower level than level 4.

⁵⁶ See footnotes 8, 9, 10, and 11.

⁵⁷ FHFA-OIG did not have prior open recommendations.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

We conducted audit fieldwork remotely from October 2022 through June 2023.

We evaluated the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines; and responded to the FY 2023 IG FISMA Reporting Metrics. Our work did not include assessing the sufficiency of internal controls over the Agency's information security programs 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 the Agency on or before July 13, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to July 13, 2023.

Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To determine if the Agency's information security programs and practices were effective, CLA conducted interviews with 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, the Agency's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, CLA compared documents, such as IT policies and procedures, to requirements stipulated in EO 14028, relevant OMB memorandums, and 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 2020 through FY 2022. See Appendix III for the status of prior year recommendations.

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

- *Government Auditing Standards* (April 2021).
- EO 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).
- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022).
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021)
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022).
- CISA's BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- FY 2023 IG FISMA Reporting Metrics (February 10, 2023).
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for specification of security controls (December 10, 2020).
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information*

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

Systems and Organizations, for the assessment of security control effectiveness.

- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (November 11, 2011).
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy*, for the risk management framework controls (December 2018).
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) (February 2014).
- Agency policies and procedures, including but not limited to:
 - *Contingency Planning Standard*, Revision 2.1 (November 30, 2022).
 - *Incident Response Standard*, Revision 2.1 (November 30, 2022).
 - *FHFA Common Control Plan* (July 16, 2021).
 - *Cyber Incident Reporting Procedures*, Revision 1.0 (December 7, 2021).
 - *FHFA Information Incident and Breach Response Plan*, Revision 5.0 (September 1, 2021).
 - *OTIM Vulnerability Management Process*, Revision 2.7 (September 7, 2022).
 - FHFA's *Supply Chain Risk Management Strategy*.
 - FHFA-OIG's *Supply Chain Risk Management Plan*.

CLA selected four FHFA systems from the total population of 37 FISMA reportable systems for testing. The four systems were selected based on risk. Specifically, four moderate categorized systems were selected, one being the FHFA GSS that supports FHFA's applications that reside on the network and the other three being systems that had not been tested in prior years. Additionally, CLA selected the OIGNet from the total population of 20 FHFA-OIG FISMA reportable 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 2023 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 the relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

STATUS OF PRIOR RECOMMENDATIONS

The table below summarizes the status of our follow-up related to the status of the open prior recommendations from the FY 2020 FISMA audit (AUD 2021-001), the FY 2021 Privacy audit (AUD 2021-011), the FY 2021 FISMA audit (AUD 2022-001), and the FY 2022 FISMA Audit (AUD 2022-009).⁵⁸

| Report #/ Finding # | Recommendation | FHFA Actions Taken | Auditor's Position on Status |
|------------------------------|--|---|---------------------------------|
| AUD 2021-001, Finding # 3 | We recommend that FHFA management: 3. Implement the planned multi-factor authentication for privileged accounts for internal systems (e.g., infrastructure). | We found that the prior year recommendation has not been resolved and remediation was in progress. Based on a review of their project plan, the estimated completion date is October 2023. | Open. |
| 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 been resolved. Management updated the PIAs using the PIA Template for AHP, FHR Navigator, and SCP. | Closed. |
| | We recommend that FHFA management: 2. Ensure PIAs are conducted timely using the PIA Template in accordance with the <i>FHFA Privacy Program Plan</i> (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 been resolved. FHFA Privacy Office updated the <i>FHFA Privacy Program Plan</i> and removed the requirement to review existing PIAs every three years. FHFA created a Continuous Monitoring schedule, scheduling reviews of PIAs. | Closed. |

⁵⁸ See footnotes 8, 9, 10, and 11.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

| Report #/ Finding # | Recommendation | FHFA Actions Taken | Auditor's Position on Status |
|------------------------------|---|---|---------------------------------|
| AUD 2021-011, Finding # 2 | <p>We recommend that FHFA management:</p> <p>3. Update the <i>Privacy Continuous Monitoring Strategy</i> to ensure that it reflects the FHFA's current privacy control assessment process in accordance with OMB Circular A-130.</p> | <p>We found that the prior year recommendation has not been resolved. We noted that the <i>FHFA Privacy Continuous Monitoring Strategy</i>, Revision 2.0 (April 29, 2022), described the control assessments conducted by the Information Security Continuous Monitoring team. However, it did not include the FHFA Privacy Office's current privacy control assessment processes such as the Privacy Office's three-year PIA review cycle and their workplan, detailing privacy control reviews and PIA reviews.</p> | Open. |
| AUD 2021-011, Finding # 3 | <p>We recommend that FHFA management:</p> <p>4. Develop and implement privacy control assessment plans that include all required elements.</p> | <p>We found that the prior year recommendation has been resolved. <i>FHFA Privacy Control Assessment Plan for Privacy Program Plan</i> (May 2, 2022) includes all required elements.</p> | Closed. |
| | <p>We recommend that FHFA management:</p> <p>5. Ensure privacy control assessments are performed for all systems that collect personal identifiable information (PII).</p> | <p>We found that the prior year recommendation has been resolved. Privacy control assessments were performed for systems that collect PII.</p> | Closed. |
| AUD 2022-001, Finding # 1 | <p>We recommend that FHFA management:</p> <p>1. Ensure that POA&M items are generated for all known system security and privacy weaknesses in accordance with NIST SP 800-37, Revision 2, and <i>FHFA's POA&M Management Procedure</i>.</p> | <p>We found that the prior year recommendation has been resolved. FHFA management tracks security and privacy weaknesses on the master POA&M spreadsheet.</p> | Closed. |

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

| Report #/ Finding # | Recommendation | FHFA Actions Taken | Auditor's Position on Status |
|------------------------------|--|--|---------------------------------|
| AUD 2022-001, Finding # 3 | <p>We recommend that FHFA management:</p> <p>2. Ensure that (a) the FHFA Information Security Incident and Personally Identifiable Information Breach Response Plan is reviewed and approved annually by the Chief Information Security Officer and Senior Agency Official for Privacy 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.</p> | <p>We found that the prior year recommendation has been resolved. The <i>FHFA Information Incident and Breach Response Plan</i> was updated and approved in March 2023. Evidence of review and approval were maintained.</p> | Closed. |
| AUD 2022-009, Finding # 1 | <p>We recommend that FHFA's Chief Information Officer:</p> <p>1.) Update the mobile devices running below the minimally acceptable operating system (OS) version or disable the devices in accordance with <i>FHFA's Mobile Device Patch Management Procedure</i>.</p> | <p>We found that the prior year recommendation has been resolved. Mobile devices are running the minimally accepted OS version or are disabled.</p> | Closed. |

**Federal Housing Finance Agency
FY 2023 Audit of FHFA’s Information Security Programs and Practices**

| Report #/ Finding # | Recommendation | FHFA Actions Taken | Auditor’s Position on Status |
|--------------------------------------|---|---|---------------------------------|
| | <p>We recommend that FHFA’s Chief Information Officer:</p> <p>2.) Formally document any risk-based decision, including compensating controls, to temporarily deviate from <i>FHFA’s Mobile Device Patch Management Procedures</i>, as necessary.</p> | <p>We found that the prior year recommendation has been resolved. Mobile devices are running the minimally accepted OS version or are disabled, and therefore, risk-based decisions were not necessary.</p> | <p>Closed.</p> |
| <p>AUD 2022-009, Finding # 2</p> | <p>We recommend that FHFA’s Chief Information Officer:</p> <p>3.) Establish and implement a process to generate and review audit log records for Legal Cost Control (LCC) Simple Invoice Management System (SIMS) on a defined basis within the Customer Controls for LCC SIMS.</p> | <p>We found that the prior year recommendation has been resolved. FHFA has decommissioned LCC SIMS.</p> | <p>Closed.</p> |

Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices

MANAGEMENTS' COMMENTS

FHFA's Management Comments



Federal Housing Finance Agency

MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audits

THROUGH: Katrina D. Jones, Chief Operating Officer

FROM: Tammy L. Tippie, Acting Chief Information Officer

SUBJECT: Draft Audit Report: Audit of the Federal Housing Finance Agency's Information Security Programs and Practices, Fiscal Year 2023

DATE: July 4, 2023

KATRINA
JONES

TAMMY
TIPPIE

Digitally signed by
KATRINA JONES Date:
2023.07.05
09:58:47 -0400
Digitally signed by TAMMY
TIPPIE Date: 2023.07.05
09:48:09 -0400

Thank you for the opportunity to respond to the above-referenced draft audit report (Report) by the Office of Inspector General (OIG), which contains 10 recommendations. This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the eight recommendations specific to FHFA in the Report. The Report also makes two recommendations (recommendations 7 and 8) specific to the FHFA OIG, who will respond in a separate memorandum.

Recommendation 1: *Update FHFA's Supply Chain Risk Management Strategy to include past due OMB M-22-18 requirements including:*

- i. *Obtaining a self-attestation from the software producer before using the software;*
- ii. *Obtaining from software producers artifacts that demonstrate conformance to secure software development practices, as needed;*
- iii. *Establishing a system to store self-attestation letters from the software producer that are not publicly available in a central location; and*
- iv. *Assessing and developing training for reviewing and validating self-attestation letters.*

Recommendation 2: *If FHFA is unable to meet the requirements in OMB Memorandum M-22- 18 in a timely manner, FHFA should consider request for an extension or waiver in accordance with OMB M-22-18. If FHFA requests a waiver, FHFA should consider documenting a risk- based decision, and document any compensating controls.*

Management Response to Recommendations 1 and 2: In September 2022, the Office of Management and Budget (OMB) released OMB M-22-18, designed to enhance the security of the federal government's software supply chain. In June 2023, OMB issued supplemental

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

July 4, 2023

Page 2 of 4

guidance, M-23-16, that extended the deadline for agencies to collect attestations from software producers and clarified the M-22-18 requirements.

FHFA agrees with the recommendations and will complete the following actions by June 30, 2024:

1. Update its Supply Change Risk Management Strategy per the OMB requirements;
2. Obtain a self-attestation from software producers;
3. Obtain, from software producers, artifacts that demonstrate conformance to secure software development practices, as needed;
4. Establish a dedicated centrally located network folder to store self-attestation letters from the software producers that are not publicly available;
5. Assess and if necessary, develop training for reviewing and validating self-attestation letters; and
6. Follow OMB guidance for attestations as it relates to non-compliant software.

Recommendation 3: *Remediate past due exploitable vulnerabilities in accordance with CISA's BOD 22-01 and the OTIM Vulnerability Management Process.*

Recommendation 4: *Develop POA&Ms to track the remediation of past due CISA known exploitable vulnerabilities that cannot be remediated in a timely manner (within 14 days) in accordance with CISA's BOD 22-01 and OTIM Vulnerability Management Process. Consider implementing compensating controls (i.e., isolating systems with un-remediated vulnerabilities) to mitigate the risk of the vulnerabilities.*

Management Response to Recommendations 3 and 4: FHFA agrees with the recommendations and will complete the following action by September 30, 2023:

1. Develop Plans of Action and Milestones (POA&Ms) to track the remediation of past due exploitable vulnerabilities known by the Cybersecurity and Infrastructure Security Agency (CISA) that cannot be remediated in a timely manner (within 14 days) in accordance with CISA's BOD 22-01 and OTIM's Vulnerability Management Process.

Recommendation 5: *Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.*

Recommendation 6: *Identify and implement solutions, in coordination with vendors, where a solution does not exist for systems to natively forward event logs to the SIEM tool. If there are no viable solutions, perform a risk assessment and cost benefit analysis. Based on the risk assessment, document any risk-based decisions, including compensating controls, for systems not in compliance with OMB M-21-31.*

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

July 4, 2023

Page 3 of 4

Management Response to Recommendations 5 and 6: FHFA agrees with the recommendations and will complete the following actions by June 30, 2024:

1. FHFA has made significant steps towards complying with OMB M-21-31 and will conduct a gap analysis to identify the outstanding requirements. The timeline to implement the remaining OMB M-21-31 requirements will depend upon availability of additional resources and funding. FHFA will draft a risk acceptance memo for OMB M- 21-31 areas that cannot be addressed.
2. Increase storage capacity to log additional applicable sources and logging categories for all Event Logging (EL) maturity tiers.
3. Implement logging capabilities to ensure applicable M-21-31 events are logged and tracked.
4. Research Security Orchestration, Automation, and Response (SOAR) and User Behavior Monitoring solutions and assess associated costs and resource impacts to FHFA.
5. Implement the strategies and tools to satisfy the OMB M-21-31 requirements.

Recommendation 9: *Review and update the Cyber Incident Reporting Procedures, and the FHFA Common Control Plan to ensure they include FHFA's three-year review cycle outlined in the Incident Response Standard.*

Management Response to Recommendation 9: FHFA agrees with the recommendation and will complete the following action by September 30, 2023:

1. Update the Cyber Incident Reporting Procedures, and the FHFA Common Control Plan to ensure they include FHFA's three-year review cycle outlined in the Incident Response Standard.

Recommendation 10: *Update the Disaster Recovery Procedures for FHFA Production Systems to include JPP and its servers, and ensure they are included in the annual contingency testing.*

Management Response to Recommendation 10: FHFA agrees with the recommendation and will complete the following action by January 31, 2024:

1. Update its Disaster Recovery Procedures for FHFA Production Systems to include the servers supporting the Correspondence Tracking System and the Job Performance Plan systems, and ensure they are included in the annual contingency testing.

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

July 4, 2023

Page 4 of 4

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

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

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

FHFA-OIG's Management Comments



OFFICE OF INSPECTOR GENERAL

Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

June 27, 2023

TO: Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP

THRU: Adam Silverman, Deputy Inspector General for Administration

FROM: Michael Smith, Chief Information Officer **MICHAEL SMITH**

SUBJECT: Draft Audit Report: Audit of the Federal Housing Finance Agency's Information Security Programs and Practices, Fiscal Year 2023

Digitally signed by
MICHAEL SMITH
Date: 2023.06.28
06:39:43 -04'00'

Thank you for the opportunity to respond to CliftonLarsonAllen's audit of the Federal Housing Finance Agency's (FHFA) and the FHFA Office of Inspector General's (FHFA-OIG) information security programs and practices for fiscal year 2023. We appreciate the audit's conclusion that FHFA-OIG's information security programs and practices were effective and complied with FISMA and related information security policies and procedures, standards, and guidelines. This memorandum provides FHFA-OIG's management response to the two recommendations applicable to our office.

Recommendation 7: *Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.*

Recommendation 8: *Identify and implement solutions, in coordination with vendors and engineering team, to encrypt logs in transit between the source system and SIEM tool. If there are no viable solutions, perform a risk assessment and cost benefit analysis. Based the risk assessment, document any risk-based decisions, including compensating controls, for systems not in compliance with OMB M-21-31.*

Management Response: FHFA-OIG agrees with Recommendations 7 and 8. As part of the existing POA&M, FHFA-OIG previously initiated actions that address these recommendations, and we expect those actions to be complete by August 27, 2023. Additionally, FHFA-OIG has implemented mitigating controls including, but not limited to, physical security controls, network access controls, multi-factor authentication system access, and network segmentation. Those mitigating controls are fully operational and accordingly the risk of unencrypted log information being intercepted is extremely low.

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

**Federal Housing Finance Agency
FY 2023 Audit of FHFA's Information Security Programs and Practices**

with FISMA legislation, OMB guidance, and NIST Special Publications. These independent audit results confirm that our Information Technology infrastructure, policies, procedures and practices are suitably designed and implemented to provide reasonable assurance of adequate security.

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

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

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