REDACTED

Federal Housing Finance Agency
Office of Inspector General

Audit of an FHFA Sensitive Employment-Related Case Tracking System: FHFA Followed its Access Control Standard, But its System Is Adversely Impacted by Two Security Control Weaknesses

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

Audit Report • AUD-2021-006 • March 29, 2021

AUD-2021-006

March 29, 2021

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency), established by the Housing and Economic Recovery Act of 2008, is responsible for the supervision, regulation, and housing mission oversight of Fannie Mae and Freddie Mac (together, the Enterprises), and the Federal Home Loan Bank System (collectively, the regulated entities). Since 2008, FHFA has served as conservator of the Enterprises.

FHFA adopted an Employment Matters Tracking System (EMT) in October 2019. EMT is an automated, searchable, and secure case tracking system used by the Agency's Office of General Counsel (OGC) and Office of Human Resources Management to track sensitive employment-related matters (e.g., matters involving conduct, performance, equal employment opportunity cases, whistleblower cases).

FHFA recognizes that strong access controls over EMT are necessary to prevent unauthorized individuals from viewing sensitive personnel information. We conducted this audit to determine whether FHFA followed its policies for access controls for EMT. Our review period was October 2019 through October 2020. For the most part, we found that FHFA followed its access control standard for granting and maintaining user access for EMT.

The [redacted] found two [redacted] security control weaknesses. FHFA is in the process of determining remedial actions for both [redacted] security control weaknesses. For this audit, we determined whether those two [redacted] weaknesses burdened the access controls for FHFA's EMT. They did. We found that FHFA did not require multifactor authentication for [redacted] to access EMT database servers. We also found that FHFA did not send EMT [redacted] for correlation and analysis. While FHFA is in the process of determining remedial actions for both [redacted] security control weaknesses, it needs to ensure corrective actions also address their impact on EMT.

Based on our findings in this audit, we make two recommendations in this report. In a written management response, FHFA agreed with our recommendations.

This report was prepared by Jackie Dang, Audit Director; David Peppers, Auditor-in-Charge; with assistance from Abdil Salah, Assistant Inspector General for Audits; and Bob Taylor, Senior Advisor. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report.

AUD-2021-006

March 29, 2021

This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov and www.oversight.gov.

Marla A. Freedman, Senior Audit Executive /s/

TABLE OF CONTENTS

ABBREVIATIONS

CUI	Controlled Unclassified Information
EMT	Employment Matters Tracking System
FHFA or Agency	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
GSS	General Support System
NIST	National Institute of Standards and Technology
OGC	Office of General Counsel
OIG	Federal Housing Finance Agency Office of Inspector General
OTIM	Office of Technology and Information Management
SIEM	Security Information and Event Management
SP	Special Publication

BACKGROUND

FHFA's Network and Systems

FHFA's network and systems process and host data and information such as financial reports, data from the Enterprises, examinations and analyses of the regulated entities, and personally identifiable information of employees. FHFA's GSS is a wide area network that provides connectivity, information sharing and data processing capabilities, remote access, and security and support services for all FHFA information systems.

FHFA's Office of Technology and Information Management (OTIM) works with mission and support offices to promote the effective and secure use of information and systems.

Standards for Access Controls

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies, including FHFA, to develop, document, and implement agency-wide programs to provide information security for the information and information systems that support the operations and assets of the agency. In addition, FISMA requires agencies to implement periodic testing and evaluation of the effectiveness of security policies, procedures, and practices. Pursuant to FISMA, the National Institute of Standards and Technology (NIST) prescribes 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. In addition, NIST issues Special Publications (SP) as recommendations and guidance documents.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, sets forth the requirements for access control, which includes account management, separation of duties,[1] least privilege,[2] and the number of unsuccessful logon attempts allowed before an account is locked. NIST also requires that the information system implements multifactor authentication for local access to privileged accounts.[3] Additionally, NIST requires that the affected organization correlates and analyzes audit records across

[1] According to NIST, separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.

[2] According to NIST, the principle of least privilege (applies to users and information system processes) ensures that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions.

[3] In this context, a privileged account is associated with a user that is authorized to perform security-relevant functions that ordinary users are not authorized to perform (e.g., network administration, database administration).

different repositories to gain organization-wide situational awareness. This requirement may be accomplished through SIEM automated tools.[4]

FHFA's Access Control Standard

FHFA's Access Control Standard, Rev. 2.1, states that access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorized use. This standard defines the security requirements needed to accomplish user access management, use of external information systems, requests for sharing information, and management of publicly accessible content. The standard helps ensure that appropriate security controls are implemented in accordance with federal requirements and information protection needs arising from other mission/business processes. The standard expects that system owners[5] will (1) determine who should have access to the information systems under their control, (2) ensure that all information they control is protected against unauthorized access, and (3) review access permissions at least annually and revise permissions based on the concept of least privilege. Specifically, FHFA's Access Control Standard requires, among other things, that:

- Users shall be granted access only to information and information systems required to perform their job function.
- Account creation requires approval by a user's supervisor, contracting officer representative, or system owner.
- Information owners and system owners shall ensure that only users with a valid need (i.e., in the performance of their official duties or duties under an authorized contract) are provided access to Controlled Unclassified Information (CUI), and that they are provided with the lowest level of access to the data (i.e., read only) necessary to perform their job function.
- System owners shall review all authorized users and privilege levels of their information systems at least annually to ensure that no users are permitted to perform incompatible functions and that access is limited based on the principle of least privilege.

[4] FHFA's Security Operations Center Strategy, version 1.4, [redacted].

[5] A system owner is an Agency official responsible for defining the operating parameters, authorized functions, and security requirements of an information system.

- Review of users with privileged accounts to the FHFA GSS shall occur at least every six months.

- Network user accounts are disabled after 35 days of inactivity.

FHFA's Employment Matters Tracking System

In 2019, FHFA adopted its EMT, which is an automated, searchable, and secure case tracking system used by the Agency's OGC and Office of Human Resources Management to track sensitive employment-related matters (e.g., matters involving conduct, performance, equal employment opportunity cases, whistleblower cases). The EMT system owner is an employee in OGC. OTIM is responsible for GSS security controls, upon which EMT relies. FHFA's Chief Information Officer signed the EMT Authority to Operate[6] memorandum on October 16, 2019.

FACTS AND ANALYSIS

FHFA Followed its Access Control Standard for Granting and Maintaining User Access for EMT; However, Two [redacted] Security Control Weaknesses, Identified in the [redacted], also Adversely Impact EMT

FHFA Followed its Access Control Standard for Granting and Maintaining User Access for EMT

FHFA developed and implemented FHFA's Access Control Standard as part of its IT security program and followed the requirements for granting and maintaining user access for EMT during the review period. Specifically, we found that:

- EMT had appropriate role-based access controls in place.[7]

- The EMT system owner approves user requests for account creation and, based on the user's role, grants user access to EMT.

[6] An Authority to Operate is the management decision given by a senior official to authorize operation of an information system and explicitly accept the risk to operations, assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

[7] Role-based access in EMT refers to assigning users to the pre-defined user roles in the system to allow individuals the ability to perform their job functions to support the Agency's mission and business goals. Lower privileged roles are restricted from viewing or modifying administrative screens such as those that allow for modification of users and permissions. These controls are applied through application controls that establish role-based permissions.

- Based on the EMT pre-defined roles, users were provided access to CUI stored within EMT and a shared folder on FHFA's network.

- The EMT system owner performed the required annual review of authorized EMT users and verified that the individuals on the list needed access granted to perform their duties.

- The EMT system owner reviewed the EMT logs of all system access activities on a [redacted] basis and followed up with OTIM Security on any irregularities or suspicious activities.

- The GSS system owner performed the required [redacted] reviews of the EMT database administrators'[8] privileged accounts.

- FHFA disabled network user accounts after [redacted] of inactivity, which included disabling access to EMT.

[redacted] *Security Weakness: FHFA Did Not Require Multifactor Authentication for [redacted] to Access EMT Database Servers*

Multifactor authentication is a control for granting users access to information technology resources only after successfully presenting two or more pieces of evidence (factors) to an authentication mechanism. Factors can include: (1) something the user knows, like a password; (2) something the user has, like a token, and (3) something the user is, like a biometric (e.g., fingerprint, retina scan).

FHFA requires multifactor authentication to log into its [redacted]. The [redacted] [9] found that FHFA's [redacted] did not always enforce multifactor authentication for local access to [redacted]. Specifically, the [redacted] found that multifactor authentication was enforced by FHFA at the [redacted] In this audit, our testing found that once the EMT [redacted] logged into the [redacted],

[8] A database administrator is charged with the creation, maintenance, backups, querying, tuning, user rights assignment, and security of an organization's databases.

[9] FISMA requires Inspectors General to perform annual independent evaluations of their respective agencies' information security program and practices to determine the effectiveness of that program and practices. For FHFA, these annual independent evaluations are performed by an independent external auditor under contract with our office. As part of these evaluations, the auditors select a sample of systems and controls to assess. In accordance with generally accepted government auditing standards, the auditors also evaluate whether FHFA has taken appropriate corrective action to address findings and recommendations from prior audits.

including the EMT database servers.[10] That finding means that multifactor authentication by the EMT [redacted] to access the EMT database server[11] was not required during the review period, in contravention of the NIST requirement.

FHFA, in response to the [redacted] finding, reported that it plans to develop an implementation and resource strategy by September 30, 2021, to address multifactor authentication for local [redacted]. While FHFA is in the process of determining remedial actions for this weakness as it applies to [redacted], it needs to ensure the corrective action also addresses EMT.

[redacted] *Security Weakness: FHFA Did Not Send EMT* [redacted] *for Correlation and Analysis*

SIEM tools are a type of centralized logging software that facilitates aggregation and consolidation of audit log records from multiple information systems. These tools facilitate audit log records correlation and analysis, which assist an organization in determining the veracity and scope of potential attacks.

FHFA's Security Operations Center Strategy, version 1.4, requires that OTIM analysts use a SIEM tool to collect audit log records from across its network. FHFA's SIEM tool is an automated tool that identifies unusual or suspicious events by themselves, or in combination with other events, across FHFA's network. Unusual or suspicious events are grouped together in dashboards, allowing OTIM analysts to more easily identify events that may require follow-up.

The [redacted] found that FHFA did not [redacted] During this audit, we found that EMT [redacted] for correlation and analysis, in contravention of FHFA and NIST requirements. FHFA, in response to the [redacted] finding, reported that it plans to assess, based on risk and other considerations, [redacted] for analysis and correlation by July 30, 2021. While FHFA is in the process of determining remedial actions for this weakness as it applies to [redacted], it needs to ensure the corrective action also addresses EMT.

[10] We found that the EMT database was encrypted, which prevented the database administrator from viewing its content. [redacted] multifactor authentication [redacted].

[11] The EMT database server is a software product that stores and retrieves data as requested by other software applications.

FINDINGS

- FHFA followed its access control standard for granting and maintaining user access to EMT.
- FHFA did not require multifactor authentication for [redacted] to access EMT database servers.
- FHFA did not send EMT [redacted] for correlation and analysis.

CONCLUSION

Strong access controls over EMT are necessary to prevent unauthorized individuals from viewing sensitive personnel information contained in EMT. We conclude that FHFA followed its access control standard for granting and maintaining user access for EMT. However, the security over EMT is impacted by two [redacted] security control weaknesses that were identified in the [redacted] audit. While FHFA is in the process of determining remedial actions for these weaknesses as they apply to [redacted], it needs to ensure the corrective actions also address EMT.

RECOMMENDATIONS

We recommend that FHFA:

1. Implement multifactor authentication for [redacted] for EMT database servers.
2. Send EMT [redacted] for correlation and analysis.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA an opportunity to respond to a draft of this audit report. FHFA provided technical comments on the draft report and those comments were considered in finalizing this report. FHFA also provided a management response, which is included in the Appendix of

this report. In its management response, FHFA agreed with our two recommendations and included the following planned corrective actions:

1. FHFA is developing a strategy to define the phased implementation strategy, testing approach, and resources required to implement multifactor authentication for [redacted], which is scheduled to be completed by September 30, 2021, which includes EMT. Strategy implementation will begin following OTIM management approval.

2. FHFA is currently performing a risk-based analysis of its collective auditing environment. This analysis includes FHFA's Security Operations Center Strategy and its ability to correlate events from various systems, which includes EMT. The analysis for the [redacted] will be completed by July 30, 2021.

We consider FHFA's planned corrective actions responsive to our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY

In light of the relative newness of EMT and sensitivity of its data, we performed this audit to determine whether FHFA followed its policies for access controls for EMT.[12] Our review period was October 2019 through October 2020.

To accomplish our objective, we:

- Reviewed NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013, updated January 2015);

- Reviewed the following FHFA policies, procedures, and related documents: Security Assessment and Authorization Process, Rev. 3.3, May 29, 2019; Access Control Standard, Rev. 2.1, dated May 22, 2020; Identification and Authentication Standard, Rev. 1.4, dated March 3, 2020; EMT Privacy Impact Assessment, dated June 7, 2019; EMT System Security Plan, Rev. 1.0, dated October 28, 2020; and GSS System Security Plan, Rev. 2.8, dated February 26, 2020;

- Reviewed and analyzed authorization and re-authorization forms listing EMT users and GSS privileged users;

[12] The [redacted] did not include EMT in its sample of systems tested. The results of our audit of EMT will inform the [redacted].

- Reviewed and analyzed EMT audit logs and evidence of the system owner's monthly review of these logs;
- Reviewed development and production versions of EMT for user access limited by roles;
- Reviewed database administrator's authentication and accessing the EMT database; and
- Interviewed officials, staff, and contractors of FHFA's OGC and OTIM regarding access controls and use of EMT.

We conducted this performance audit between October 2020 and March 2021 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 objective.

APPENDIX: FHFA MANAGEMENT RESPONSE.....

Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Senior Audit Executive

FROM: Kevin Smith, Chief Information Officer KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2021.03.18 15:08:55 -04'00'

SUBJECT: Draft Audit Report: *Audit of an FHFA Sensitive Employment-Related Case Tracking System: FHFA Followed its Access Control Standard, But its System Is Adversely Impacted by Two Security Control Weaknesses*

DATE: March 11, 2021

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

Recommendation 1: *Implement multifactor authentication for* [redacted] *for EMT database servers.*

Management Response: FHFA agrees with Recommendation 1. As discussed in FHFA's management response to the [redacted], FHFA is developing a strategy to define the phased implementation strategy, testing approach, and resources required to implement multifactor authentication for [redacted], which is scheduled to be completed by September 30, 2021. Strategy implementation will begin following OTIM management approval, which will include EMT.

Recommendation 2: *Send EMT* [redacted] *for correlation and analysis.*

Management Response: FHFA agrees with Recommendation 2. As discussed in FHFA's management response to the [redacted], FHFA is currently performing a risk-based analysis of its collective auditing environment. This analysis includes FHFA's Security Operations Center Strategy and its ability to correlate events from various systems, which includes EMT. The analysis [redacted] will be completed by July 30, 2021.

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

CC: Chris Bosland
Kate Fulton
Ralph Mosios
John Major
Janice Kullman

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