Federal Housing Finance Agency
Office of Inspector General

# FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats

Audit Report • AUD-2024-007 • August 12, 2024

# ............................. EXECUTIVE SUMMARY ............................

## PURPOSE

As part of our ongoing oversight of the Federal Housing Finance Agency's (FHFA or Agency) implementation of the Federal Information Security Modernization Act (FISMA), we perform audits of networks and information security of the Agency. Our objective for this audit was to determine whether the Agency's security controls were effective to protect its network and systems against internal threats from October 2023 through January 2024.

## RESULTS

We determined that FHFA's security controls were not effective to protect its network and systems against internal threats. Our penetration testing demonstrated that the Agency's network has serious vulnerabilities that increase the likelihood that hacking attempts will succeed. In one instance, we gained access to a privileged user account that allowed us to view, edit, or save files on the local drives of any user's laptop or desktop, including FHFA executives at the highest levels. We were also able to elevate a standard user account to a domain administrator and take full control of FHFA's network. We essentially had unfettered access to the Agency's information technology (IT) infrastructure.

These vulnerabilities make FHFA's IT infrastructure and the sensitive information stored on it more susceptible to unauthorized access and security compromises. The breadth, depth, and potential impact of the network security deficiencies are serious matters that require prompt corrective action by FHFA management. Accordingly, we are reporting eight findings related to the identified control deficiencies.

## RECOMMENDATIONS

We made 22 recommendations to address our findings. In a written response, FHFA management agreed with our recommendations.

This report was prepared by Zachary Lewkowicz, IT Audit Manager; Brian Prisbe, IT Specialist; with assistance from Abdil Salah, Assistant Inspector General for Audits. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report. 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.

James Hodge
Deputy Inspector General for Audits /s/

# TABLE OF CONTENTS ........................................................

# ABBREVIATIONS

| | |
|---|---|
| BOD | Binding Operating Directive |
| CISA | Cybersecurity & Infrastructure Security Agency |
| CUI | Controlled Unclassified Information |
| CVSS | Common Vulnerability Scoring System |
| DLP | Data Loss Prevention |
| Enterprises | Fannie Mae and Freddie Mac |
| FHFA or Agency | Federal Housing Finance Agency |
| FISMA | Federal Information Security Modernization Act of 2014 |
| GAO | Government Accountability Office |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| OIG | Federal Housing Finance Agency Office of Inspector General |
| OTIM | Office of Technology and Information Management |
| PII | Personally Identifiable Information |
| PIV | Personal Identity Verification |
| SP | Special Publication |
| USB | Universal Serial Bus |

# BACKGROUND

FISMA requires agencies, including FHFA, to develop, report, and implement agency-wide programs to provide 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 their 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. Those information security standards provide minimum information security requirements necessary to improve the security of federal information and information systems. In addition, NIST develops and issues recommendations and guidance documents called Special Publications (SP).

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

- Maintain and enhance the resilience and availability of IT resources and systems;
- Provide support, and secure IT resources, services, and data needed to support research and analysis of the regulated entities and the housing markets;
- Ensure FHFA implements an effective information security program consistent with requirements highlighted in FISMA;
- Identify technologies and tools to increase the productivity and efficiency of FHFA staff; and
- Create and maintain an IT Strategic Plan that addresses current, and adapts to future, IT needs.

FHFA's network and systems host a variety of data and information such as financial reports and data from Fannie Mae and Freddie Mac (the Enterprises), Common Securitization Solutions, LLC, the Federal Home Loan Banks, and the Office of Finance, as well as FHFA employees' personally identifiable information (PII). As such, it is important that the configurations and controls in place are effective to prevent unauthorized access to systems and information. If unauthorized access to FHFA's network is successful, attackers may have ample opportunities to compromise the confidentiality, integrity, and availability of FHFA's sensitive information. For example, attackers can extract, delete, or modify sensitive data, including PII; discover usernames and passwords; and launch denial-of-service attacks.[1] If these unauthorized activities are not timely detected or prevented, such activities could result in compromises of systems and information, hindering FHFA's mission. To protect against these vulnerabilities, FHFA has implemented a security program that includes security testing and assessments for determining the effectiveness of security controls in safeguarding its information systems and controlled unclassified information (CUI).[2]

## OBJECTIVE AND SCOPE

The objective of our audit was to determine whether FHFA's security controls were effective to protect its network and information systems against internal threats.[3] The audit scope covered FHFA's internal network and information systems from October 2023 through January 2024. This work will support the annual FISMA evaluation of FHFA's security program and practices.

## RESULTS

We determined that FHFA's security controls were not effective to protect its network and systems against internal threats. Specifically, FHFA did not consistently apply all required security controls over FHFA's network and systems. To test controls intended to thwart internal threats, FHFA gave us the typical access provided to any FHFA employee (i.e., an FHFA-issued laptop computer and a standard user account), as well as network access for FHFA Office of Inspector General (OIG) test laptops.[4] Our penetration testing demonstrated that the Agency's

[1] NIST defines a denial-of-service attack as an attack meant to shut down a system or network making it inaccessible to its intended users.

[2] NIST defines CUI as information required by law, regulation, or government-wide policy to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information (December 29, 2009), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

[3] An internal or insider threat is a current or former employee, contractor, or other business partner who has or had authorized access to a network, system, or data, and intentionally exceeds or misuses that access, resulting in a negative effect on the organization's information security.

[4] Consistent with NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* (September 30, 2008), we signed Rules of Engagement with FHFA management. Among other things, the Rules of Engagement defined the target systems, scope, test methodology, test schedule, points of contact, data handling, and notification methods for the internal penetration test. FHFA also agreed to authorize our OIG test laptops to connect to the FHFA network and agreed to not intentionally block or diminish OIG access. Additionally, FHFA agreed that if an alert were triggered, FHFA would help remediate any blocked or diminished access situations resulting from our test. However, as stated in the Rules of Engagement, the document does not limit the authority of OIG to conduct audits in accordance with the Inspector General Act of 1978, as amended.

network has serious vulnerabilities that increase the likelihood that hacking attempts will succeed.

Using the FHFA-issued laptop computer and standard user account, we gained access to sensitive information, including PII, stored on FHFA's network that should have been restricted. We were able to run unapproved portable programs and scripts, which we used to enumerate (systematically probe for certain information) FHFA's users and computers and obtain information on when users last changed their passwords. We found that OTIM used two standard default passwords to set up all FHFA user accounts and that some standard users did not change their default passwords. We accessed some users' sensitive data using the default passwords. Additionally, we transferred mock sensitive user information both by email and upload to cloud-based storage services.

With the penetration testing tools installed on the OIG test laptops, we were able to search for FHFA employees who were using their default passwords. We discovered that 178 standard users and 1 privileged user did not change their initial default password. The usernames and default passwords gave us access to some users' sensitive data without their knowledge. Additionally, the privileged user account allowed us to view, edit, or save files on the local drives of any user's laptop or desktop, including those of FHFA executives at the highest levels. With privileged access, we also found unencrypted credentials to FHFA's cloud environment on the local drive of a cloud administrator's computer.

Once we gained access to the cloud environment, we had permissions to execute commands on FHFA's cloud computers. Using remote commands, we added one of our FHFA assigned user accounts to the domain admin group that gave us full control of the FHFA network. We had unfettered access to all users and computers, including those of FHFA executives at the highest levels. We also had the ability to create, delete, and modify users, computers, and groups across the internal domain. After gaining access to a privileged user account, we were able to transfer large amounts of sensitive user information, including email files (i.e., emails, attachments, address books, and calendars), configuration files, and documentation for internal IT systems to one of our OIG test laptops. FHFA did not detect us transferring files and information over its network. Furthermore, we found vulnerabilities in FHFA's networks that our penetration testing tool was unable to exploit.

As part of our testing of internal threats, we assessed employee adherence to physical security over information and computer assets. We were able to view sensitive information on employees' laptops because users did not adhere to their responsibility to lock unattended devices. Furthermore, FHFA's security controls did not restrict or prohibit us from attaching an unauthorized device to extract sensitive information from FHFA laptops. Moreover, FHFA did not update its Common Control Plan[5] for wireless networks' configurations.

These vulnerabilities make FHFA's information technology infrastructure and the sensitive information stored on it more vulnerable to unauthorized access and security compromises. We consider the breadth, depth, and potential impact of the network security deficiencies as serious matters that require prompt corrective action by FHFA management. In all, we are reporting eight findings:

1. OTIM did not effectively implement least privilege controls.
2. OTIM did not effectively manage user authentication for access to FHFA's systems.
3. OTIM did not use secure methods to access FHFA's cloud environment.
4. OTIM did not effectively enforce information flow control within FHFA's network and to the internet.
5. OTIM did not detect and prevent standard users from downloading and installing unapproved software from the internet (repeat finding).
6. OTIM did not remediate vulnerabilities in FHFA's systems.
7. Physical security controls within FHFA's headquarters building did not prevent access to offices and employee information (repeat finding).
8. OTIM did not update FHFA's Common Control Plan for wireless configurations.

## Finding 1: OTIM Did Not Effectively Implement Least Privilege Controls

We found that OTIM did not effectively implement least privilege controls to restrict access to sensitive information stored in some folders on FHFA's network. NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, requires that organizations only allow user access necessary to accomplish assigned tasks in accordance with missions and business functions. Furthermore, FHFA's Access Control Standard, Revision 2.3 (November 30, 2022), requires that FHFA users are provided with the lowest level of access to the data necessary to perform their job functions.

Using our assigned FHFA laptop and standard user access rights, we accessed a number of folders on FHFA's network that contained sensitive information. Specifically, we accessed

[5] The purpose of this Common Control Plan is to document FHFA's organizational implementation of NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* controls.

onboarding hiring forms and spreadsheets that contained first and last names, social security numbers, addresses, phone numbers, security clearance status, and other sensitive information. In addition, we obtained daily visitor logs to FHFA headquarters, floor plans for FHFA headquarters, internal organization codes, resumes, and budget planning files. Lastly, we identified a folder marked "to be deleted" that contained private emails from FHFA senior management officials regarding an equal employment opportunity office complaint.

We also accessed a log file on FHFA's network that was generated by an OTIM developed software script. The log file contained FHFA users' login information (e.g., login date, login time, username, computer name, computer description, and Internet Protocol (IP) address).

When we presented our network access findings to OTIM officials, they stated that OTIM enables users to set permissions on the folders they own because the owners are most knowledgeable about who should be given access. OTIM does not require users to request folder permissions through a help desk ticket. OTIM officials explained that as a consequence, non-IT staff made mistakes in applying permissions to the folders. When we asked if non-IT staff were ever trained on how to set up folder permissions, we were told that training was probably provided over a decade ago, and there were no records of that training. Additionally, OTIM officials told us that they conduct annual training on how to safeguard CUI, but that training does not cover managing folder permissions.

OTIM officials explained that users needed to have "read and write" permissions[6] for the log file. This access allowed the software to track and record each user's login times and the operating systems they were using. Officials told us that exposure of the log file did not present any risk because the same information could be gathered by a standard user on FHFA's internal network. In a meeting, we disclosed to OTIM that we were able to use the log file as an internal roadmap to see where specific users were logging in. After explaining the risk of having access to this sensitive information, OTIM officials told us they deleted all the log files and the software script will no longer generate log files. We did not validate OTIM's assertion because OTIM did not provide us with requested evidence showing that these actions were taken.

OTIM's lack of adherence to NIST and FHFA's standards on least privilege creates a risk for unauthorized access to FHFA's sensitive information as demonstrated during our testing. In a malicious attack, employees' identities could be stolen, causing victims serious financial and emotional distress. Furthermore, the disclosure of this information could cause public embarrassment and reputational damage to the Agency. Additionally, an insider could use the information in the computer log file to enumerate FHFA users and track which computers they

[6] Read permissions give authority to open and read a file. Write permission give authority to modify the contents of a file.

use.  This information could further be leveraged by an insider to cause disruption to FHFA's network operations and services.

### Recommendations

We recommend that the FHFA Chief Information Officer:

1. Restrict user access to the folders and files on FHFA's network in accordance with least privilege principle.

2. Evaluate the need for the software script to generate and record user login records and restrict access to the log files in accordance with least privilege principle.

## Finding 2: OTIM Did Not Effectively Manage User Authentication for Access to FHFA's Systems

We found that some standard users did not change their default passwords.  With that knowledge, we accessed sensitive data using their compromised credentials.  Multifactor authentication[7] was not required.  Additionally, we were able to access files on FHFA's network that our standard user account did not have permission to access, including files containing sensitive information.  For example, we accessed sensitive files of different offices within FHFA using the compromised credentials.

With penetration testing tools, we were able to search for employees who were using default passwords.  We found that 178 standard users and 1 privileged user did not change their default passwords.  The privileged user working the IT helpdesk had a standard user account and a privileged account with the same password.  We found that the privileged user could view, edit, or save files on the local drives of any user's laptop or desktop without the user's knowledge.

We used the information in the network log file, noted in the previous finding, to identify where specific users were logging in.  On multiple occasions, we accessed local files on the laptops of high-level FHFA executives and transferred email files and other personal files to one of our OIG test laptops.  We also found that the privileged user account could modify permissions for other standard user accounts.  We used the privileged user account to elevate our standard user account to a higher access level, which granted us more permissions.  FHFA had controls in place to detect when we performed this activity and notified us, but did not stop us due to parameters agreed upon for our testing.

[7] Multifactor authentication, as defined by NIST, is authentication using two or more factors to achieve authentication.  Factors are (i) something you know (e.g., password or personal identification number); (ii) something you have (e.g., cryptographic identification device, token); and (iii) something you are (e.g., biometric).

NIST SP 800-53 Rev. 5 requires organizations to manage passwords for users and devices by establishing initial passwords that meet password strength requirements. Furthermore, FHFA's Common Control Plan requires that upon first login, account management settings ensure that the new user establishes a password that meets FHFA requirements for length and complexity and that the password is not a commonly used or a known compromised password. Additionally, the Common Control Plan requires that passwords for privileged accounts should be different than the passwords for the user's standard account and should be set to "User must change password at next logon" when created by OTIM engineers.

OTIM officials told us password procedures were not being properly followed, and that prior to our testing, they were aware that some users were using default passwords and had asked users to change them. However, OTIM officials were not aware that the helpdesk was setting up accounts with a second default password and did not ask all users to change their passwords. OTIM officials noted that even for users who were forced to change their password, they were only making minor changes, such as adding one character to the beginning or end.

OTIM officials also explained that there is a feature to force users to reset their passwords, but if the user uses a personal identity verification (PIV) card,[8] the feature to force the password reset is bypassed. OTIM deemed it irrelevant to force this feature because nearly everyone uses a PIV card. Instead, OTIM officials said they are looking to implement a solution that all users receive a different complex password for initial login. OTIM officials also noted that a standard user or privileged user can access FHFA network drives without using PIV or multifactor authentication because that is the default behavior for network drives. They stated that, to the best of their knowledge, there is no mechanism to require multifactor authentication on network drives. Access control weaknesses may increase the risk of unauthorized access to FHFA's systems and data.

These kinds of access control weaknesses may increase the risk of unauthorized access to FHFA's systems and data. By leaving initial default login passwords unchanged, an insider could gain unauthorized access to sensitive information and privileges of any compromised users, including that of a privileged user. This access could be further used to extract sensitive or personal information from any FHFA user without being detected. Moreover, the lack of multifactor authentication controls could allow an insider to gain unauthorized access to FHFA's network and exfiltrate sensitive information from the network. An attacker could use this information to conduct identity theft and social engineering of FHFA users.

[8] NIST defines PIV cards as a physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so the claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

In accordance with our Rules of Engagement, we did not attempt to perform actions that would disrupt FHFA's operations, such as deleting data, powering off servers or other resources, locking out accounts, and similar activities, any of which could have resulted in interruption or shutdown of devices or services. However, malicious attackers would have no such restrictions against performing these actions.

### Recommendations

We recommend that the FHFA Chief Information Officer:

3. Ensure that the default or initial login passwords are changed for all 179 users whose passwords were compromised in this audit.

4. Ensure that upon initial login, FHFA users establish a new password that meets FHFA requirements for length and complexity and that the password is not a commonly used or a known compromised password.

5. Ensure that standard user accounts and privileged user accounts are not set up with the same default or initial login password.

6. Ensure that personnel are trained on standard and privileged user FHFA authentication and identification policies.

7. Identify and implement a solution, in coordination with vendors, to ensure that multifactor authentication is required to access FHFA's network. If there are no viable solutions, document any risk-based decisions, including compensating controls.

## Finding 3: OTIM Did Not Use Secure Methods to Access FHFA's Cloud Environment

We found that FHFA's access to its cloud environment was not secure. Specifically, using the privileged account that we compromised as noted above, we accessed an FHFA cloud administrator's laptop. We found that the cloud administrator used an unsecure access method that stored plaintext credentials (i.e., unencrypted) to FHFA's cloud environment. Using these credentials, we accessed FHFA's cloud environment and were not required to use multifactor authentication. We were able to run remote commands to elevate one of our FHFA-assigned standard user accounts to a domain administrator, thereby gaining full control of FHFA's network. We had permissions to do anything on FHFA's network, including viewing what was running on users' desktops, saving and deleting files on file servers, and adding or deleting user accounts. FHFA had controls to detect when we elevated our standard user account to a domain administrator and notified us, but these controls did not detect or prevent us from accessing FHFA's cloud environment in the first place.

As a best practice, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) recommend that organizations avoid creating credentials with administrative privileges. Credentials should never be included in plain text; instead, they should be handled securely by a secrets manager[9] and stored with encryption.[10] Multifactor authentication for users, such as one-time passwords or smartcards, should be implemented where possible.

Each cloud service provider offers different options for obtaining and managing credentials, so it is best to periodically review their guidance. We reviewed FHFA's cloud service provider guidance, which states that to avoid security risks, organizations should not use unsecure access methods that store plaintext credentials for accessing the cloud environment.

OTIM officials explained that the cloud administrator used an unsecure access method because it streamlined operations. Additionally, OTIM officials were not aware of multifactor authentication methods that could be used to securely authenticate to the cloud environment. However, as noted above, using this unsecure access method allowed us to do anything we wanted on FHFA's network, essentially giving us unfettered access to the Agency's IT infrastructure.

Allowing privileged users to access FHFA's cloud environment without multifactor authentication increases the risk of unauthorized access or compromise of cloud resources. An attacker could run remote commands on FHFA's cloud servers to elevate privileges and take over FHFA's entire network. With domain administrator access, a perpetrator could delete or modify FHFA's data, resulting in a loss of confidentiality, integrity, and availability, and could conduct a ransomware attack to further disrupt FHFA's operations. Without proper detection, an attacker could persistently remain on the network to conduct further malicious activities.

### Recommendations

We recommend that the FHFA Chief Information Officer:

8. Change the credentials for the compromised cloud administrator account.

9. Use the secure access method recommended by FHFA's cloud service provider to access the FHFA cloud environment.

[9] A secrets manager is an application or service used to manage, retrieve, or rotate credentials.

[10] CISA and NSA, *Use Secure Cloud Identity and Access Management Practices*, Ver. 1.0 (March 2024), provide organizations with recommended best practices or mitigations to improve the security of their cloud environment(s).

10. Identify and implement a solution, in coordination with vendors, to ensure multifactor authentication is required for privileged users to access FHFA's cloud environment. If there are no viable solutions, document any risk-based decisions, including compensating controls.

## Finding 4: OTIM Did Not Effectively Enforce Information Flow Control Within FHFA's Network and to the Internet

We used our standard user access rights as FHFA employees to transfer files containing sensitive user information, including onboarding investigation files with PII, from network drives to both our assigned FHFA laptop and one of our OIG test laptops. After gaining access to a privileged user account, we also successfully transferred large volumes of sensitive information to the same OIG test laptop. This information included email files (i.e., emails, attachments, address books, and calendars) along with configuration files and documentation for internal IT systems.

As described below, our testing demonstrated that standard users are capable of moving sensitive documents to personal accounts on cloud-based email and storage services.

- Using the assigned FHFA laptop and a standard user account, we sent a mock document file containing fictitious CUI and marking to a mock non-government email account. We also sent a spreadsheet file containing fake PII (i.e., first names, last names, and social security numbers) to the same account. These files were accessible outside of FHFA's network.

- Using the same setup above, we transferred the aforementioned mock document and spreadsheet files to two different cloud storage services. These files were accessible outside of FHFA's network.

NIST SP 800-53 Rev. 5 requires that organizations enforce approved authorizations for controlling the flow of information within the system and between connected systems based on organization-defined information flow control policies. Additionally, in accordance with FHFA's Rules of Behavior, users are prohibited from sending CUI to a non-government email account, regardless of whether the information is marked as CUI. This includes, but is not limited to, emails, files, and meeting invitations related to official FHFA business. FHFA users are also prohibited from transferring CUI to any unauthorized external file hosting service or posting CUI to a public website.

OTIM officials stated that FHFA's intrusion prevention system[11] sits at the network perimeter and does not detect or block traffic that is moving across the internal network. For email, OTIM

[11] An intrusion prevention system can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target(s).

officials stated they do not have real time monitoring and that they only monitor for messages exceeding a certain size.  Messages exceeding the size limit are sent to the security team’s mailbox to determine if CUI is going to an unauthorized recipient.  For cloud storage, OTIM officials said that they have some capability to block transfer of CUI to cloud storage, but they do not have a data loss prevention system in place to block every instance.  The same officials stated that they do not have the resources required to implement a data loss prevention system. Additionally, OTIM officials noted that they cannot prevent users from logging in to their personal cloud storage accounts.

Ineffective control over the flow of information enables users to transfer sensitive information, including CUI and PII, and large data files outside of FHFA’s network without being detected and prevented as demonstrated in our testing.  Consequently, FHFA is at risk of unauthorized disclosure or compromise of sensitive information that could cause significant damage to the Agency.  This includes the potential for identify theft, financial fraud, and emotional distress for those affected.

### Recommendations

We recommend that the FHFA Chief Information Officer:

11. Identify and implement a solution to detect and monitor the transfer of large amounts of data moving across FHFA’s network.

12. Identify and implement a solution to detect and prevent controlled unclassified information or personally identifiable information from being transferred outside of FHFA’s network to personal accounts on email and cloud-based storage services.

13. Determine whether resources can be made available to implement a data loss prevention system to prevent the exfiltration of controlled unclassified information.

## Finding 5: OTIM Did Not Detect and Prevent Standard Users from Downloading and Installing Unapproved Software from the Internet (Repeat Finding)

We used our FHFA assigned laptop and standard user account to download and run a script from the internet to extract a list of all computers on FHFA’s network.  We also downloaded and ran a portable program[12] to extract additional information from FHFA’s network (e.g., user’s last login, time of user’s last password reset, user groups and privileges, etc.).  FHFA did not detect and prevent us from downloading and running these unapproved software programs.  However,

[12] Portable programs are designed to be self-contained programs and can run from wherever they are stored (i.e., they do not need to be installed into a computer’s operating system to run).  Portable programs can, for example, be run from a flash drive or from a computer’s hard drive.

FHFA was able to block us from installing some hacking tools and other programs we attempted to use to escalate privileges, extract password hashes, and run interception attacks.

NIST SP 800-53 Rev. 5 requires organizations to enforce software installation policies through organization-defined methods and to monitor policy compliance. Furthermore, FHFA's Common Control Plan states that automated monitoring tools are in place to track and monitor any changes or software download attempts. According to the Common Control Plan, firewall logs are reviewed daily (every business day) to identify software downloaded to the network. In accordance with FHFA's Rules of Behavior, users are prohibited from installing hardware, software, web-browsers, plugins and extensions, or peripherals on FHFA IT equipment unless authorized by OTIM.

OTIM officials stated that they did not detect or prevent standard users from downloading and running unapproved software programs or monitor and respond to software download attempts because the former Acting Chief Information Officer accepted these risks in December 2020 after they were identified in our 2019 audit report.[13] OTIM officials noted that the security tools they have in place have known limitations and are not able to block all portable programs because they do not need to be installed on the computer's operating system to run. OTIM does have security controls in place to block unauthorized programs from being installed in specific folders and when malicious activity is detected. OTIM officials also stated that they allow for certain scripts to run and they have tools in place to look for executable programs performing abnormal activities.

This finding was previously identified in our 2019 audit report. At that time, FHFA's former Acting Chief Information Officer accepted the risks associated with not installing an automated application to block users from downloading and running unapproved software. As such, the recommendation was closed. However, this risk acceptance requires re-evaluation given the breadth, depth, and potential impact of the vulnerabilities identified. Unauthorized download and operation of unapproved software without detection or prevention exposes FHFA's network and systems to potential attacks. We demonstrated this internal threat exposure using unauthorized programs and utilities on our assigned FHFA laptop to conduct information gathering for our penetration test. An employee or contractor could potentially download malicious programs that could harm FHFA's network and systems and further lead to the compromise of sensitive data or loss of operations.

### Recommendations

We recommend that the FHFA Chief Information Officer:

[13] *See* OIG, *2019 Internal Penetration Test of FHFA's Network and Systems* (AUD-2019-014, September 24, 2019).

14. Reevaluate the former Acting Chief Information Officer's risk acceptance related to portable software programs, and implement security controls to detect and prevent users from downloading and running unapproved software on FHFA's system in accordance with NIST and FHFA's Rules of Behavior.

15. Monitor and respond to unauthorized software downloads in accordance with FHFA's Common Control Plan.

## Finding 6: OTIM Did Not Remediate Vulnerabilities in FHFA's Systems

We found that OTIM did not remediate vulnerabilities, including critical ones, as quickly as FHFA policy requires. The OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022), has established target remediation timeframes based on the vulnerability severity rating. The process requires that internal critical exploitable[14] vulnerabilities are remediated within 90 days, internal high exploitable within 120 days, and internal medium exploitable within 180 days. Furthermore, the process requires that CISA Known Exploitable Vulnerabilities are remediated within 14 days.

Using one of our OIG test laptops, we performed vulnerability scans[15] of FHFA's internal network and identified 3,318 total vulnerabilities that our scanning tool evaluated as potentially exploitable on FHFA's servers, workstations, and other devices. Of the total vulnerabilities identified, 2,107 (64 percent) were critical, 901 (27 percent) were high, and 310 (9 percent) were medium.[16] In addition, 2,116 of the 3,318 (64 percent) total exploitable vulnerabilities were over one year old. These exploitable vulnerabilities included 1,252 (59 percent) that were critical, 632 (30 percent) that were high, and 232 (11 percent) that were medium.

Of the 3,318 total exploitable vulnerabilities, 261 (8 percent) were identified as CISA Known Exploitable Vulnerabilities. Of the 261 CISA Known Exploitable Vulnerabilities, 224 (86 percent) were critical, 26 (10 percent) were high, and 11 (4 percent) were medium.

[14] According to the OTIM Vulnerability Management Process, exploitable vulnerabilities are those with an active working exploit that is publicly available in tools and represents the highest risk. On the other hand, non-exploitable vulnerabilities are those without a known active working exploit and, therefore, pose a lower risk.

[15] Vulnerability scanning is a security technique used to identify security weaknesses in a computer system. Vulnerability scanning can be used by individuals or network administrators for security purposes, or it can be used by hackers attempting to gain unauthorized access to computer systems.

[16] Computer security vulnerabilities are rated using the NIST Common Vulnerability Scoring System V3 ratings (CVSS), a 10-point scale based on the likelihood and consequences of someone exploiting the vulnerability. CVSS base scores 9.0 or higher are critical severity, 7.0 to 8.9 are high severity, 4.0 to 6.9 are medium severity, and 0.1 to 3.9 are low severity, with a score of 0 representing a severity level of none.

Furthermore, 168 (64 percent) were over one year old [158 (94 percent) were critical and 10 (6 percent) were high].

NIST SP 800-53 Rev. 5 requires that organizations monitor, scan, and remediate vulnerabilities in systems and applications within organizationally defined timeframes and processes.

CISA's Binding Operating Directive (BOD)[17] 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.

We provided the results of our vulnerability scanning to OTIM during fieldwork. OTIM officials stated that they did not have the time or resources to compare our scanning results with the results from their own vulnerability scanning tool. OTIM informed us that they are constantly doing patch management and it consumes much of their time. OTIM officials also stated that some machines are no longer being patched, and there are risk acceptances for those machines. However, OTIM did not provide evidence of which vulnerabilities were attributable to the machines with risk acceptances. Lastly, OTIM officials stated that some machines are more complicated to patch because they may stay offline for long periods of time, and patches require testing before being implemented. At a minimum, OTIM should have remediated the 261 Known Exploitable Vulnerabilities within 14 days as required by CISA.

FHFA's lack of adherence to FHFA policy on security vulnerability mitigation puts servers and workstations, information systems, and sensitive information at risk for compromise. Specifically, an insider could exploit vulnerabilities to take control of systems and cause a denial-of-service attack or allow unauthorized access and malicious modification to FHFA's systems and data. In addition, vulnerabilities that remain un-remediated over an extended period of time increase FHFA's exposure and the likelihood that the confidentiality, integrity, and availability of FHFA systems and data could be compromised.

### Recommendations

We recommend that the FHFA Chief Information Officer:

16. Identify and secure the resources necessary to remediate identified internal critical, high, and medium exploitable vulnerabilities on the FHFA servers, workstations, and

[17] 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.

other devices in compliance with CISA BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022).

17. Develop a Plan of Action and Milestones to track the remediation of past due CISA Known Exploitable Vulnerabilities in accordance with CISA's BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022). OTIM should implement compensating controls (i.e., isolating systems with un-remediated vulnerabilities) to mitigate the risk of the vulnerabilities.

18. Prioritize existing OTIM resources based on the Plan of Action and Milestones to ensure that CISA Known Exploitable Vulnerabilities are remediated in accordance with CISA's BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022).

## Finding 7: Physical Security Controls Within FHFA's Headquarters Building Did Not Prevent Access to Offices and Employee Information (Repeat Finding)

FHFA did not effectively enforce device lock controls to automatically lock FHFA laptop screens after 15 minutes of inactivity in accordance with FHFA policy. In addition, FHFA users did not adhere to their responsibility to lock unattended devices as required in the FHFA Rules of Behavior. Specifically, we found two unattended laptops that were left unlocked in an area accessible to all employees of FHFA's headquarters building. One laptop was being used for a presentation and the other was playing a video file. We were able to access the logged in users' email accounts, personal files, and network drives on both laptops. We came back an hour later and found the devices remained unlocked. There were no controls applied to prevent unauthorized individuals from accessing, reading, copying, deleting, altering, or stealing FHFA data. Additionally, FHFA's security controls did not restrict or prohibit us from attaching an unauthorized device to a universal serial bus (USB)[18] port to capture sensitive information from FHFA laptops.

NIST SP 800-53 Rev. 5 requires that organizations prevent further access to systems by initiating a device lock after an organization-defined time period of inactivity or by requiring the user to initiate a device lock before leaving the system unattended. NIST also requires that organizations restrict or prohibit the use of organization-defined types of system media on organization-defined systems or system components using organization-defined controls.

FHFA System Security and Privacy Plan for the General Support System (June 5, 2023) states that laptops automatically enforce screen saver locks after 15 minutes of inactivity. Additionally, FHFA's Rules of Behavior state that it is a user's responsibility when leaving

[18] NIST defines a USB as a type of standard cable, connector, and protocol for connecting computers, electronic devices, and power sources.

the workstation, regardless of location, to activate the lock screen on the computer to prevent unauthorized individuals from accessing, reading, copying, deleting, altering, or stealing FHFA information. Users are also responsible for physically securing FHFA equipment when it is not in their possession. In addition, unless authorized by OTIM, users are prohibited from attaching any unauthorized computing storage device (e.g., flash memory cards, USB thumb drives, portable disk drives, tablets, mobile phones, or digital cameras) to any FHFA IT device or the FHFA network and installing hardware or peripherals on FHFA IT equipment.

For one laptop left unattended, OTIM officials stated that FHFA approved an exception of the screensaver timeout settings that is limited to workstations used for audio or visual presentations and conferences. Furthermore, FHFA has accepted the risk associated with the technical limitation that prevents the screen from locking after 15 minutes of inactivity if a video is playing. However, this risk acceptance requires re-evaluation given the breadth, depth, and potential impact of the vulnerabilities identified. For the second unattended laptop, OTIM officials explained that this was a failure of the respective user to follow Agency policy. Regarding the attachment of an unauthorized device to a laptop, OTIM officials stated that their security controls would not be able to detect it because our device did not show up on the list of USB devices or use any drivers.

This finding was previously identified in our 2019 report. At that time, FHFA management agreed with our recommendation and took actions to train and enforce employee's responsibilities to secure sensitive information. As such, the recommendation was closed. FHFA's weaknesses in physical security create the risk that attackers, including insiders, can capture sensitive data on FHFA's computers, such as usernames, passwords, and PII, and use this information to gain unauthorized access to FHFA's systems. Furthermore, lack of user adherence to the FHFA Rules of Behavior for locking unattended workstations creates a risk for unauthorized access to FHFA sensitive information. Those with physical access to FHFA headquarters could access, read, copy, delete, or alter information on FHFA's network. Additionally, ineffective security controls over access to facilities and USB ports on laptops creates a risk for unauthorized access to sensitive information, as demonstrated during our testing.

### Recommendations

We recommend that the FHFA Chief Information Officer:

19. Reevaluate the former Chief Information Officer's risk acceptance related to the device lock policy and implement security controls to ensure that all FHFA laptops adhere to FHFA's device lock policy in accordance with FHFA System Security and Privacy Plan for the General Support System (June 5, 2023).

20. Emphasize through training an FHFA user's responsibility to securely lock their unattended devices.

21. Implement security controls to lock down USB ports so that only authorized USB devices are allowed.

## Finding 8: OTIM Did Not Update FHFA's Common Control Plan for Wireless Configurations

We found that one of FHFA's wireless networks was broadcasting (i.e., available to join) contrary to FHFA's Common Control Plan. According to the plan, this particular wireless network is supposed to be set to non-broadcast, which means it should not appear in a list of available wireless networks unless it is specifically configured on the device. In contravention of FHFA's plan, we were able to see the name of the network in a list of wireless networks in range when conducting our scans of FHFA's wireless networks from a host not specifically configured by FHFA.

OTIM officials explained that the wireless network in question was set to broadcast mode in accordance with an approved change request in 2019 to resolve issues with cellphones connecting to the wireless network. OTIM officials stated that the information in the Common Control Plan is inaccurate and should be updated.

According to the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government,*[19] management should periodically review policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. Management should promptly review any significant changes in an entity's process to determine that the control activities are appropriately designed and implemented.

By not updating its Common Control Plan to reflect its wireless configurations, FHFA risks that its plan may result in inconsistencies that do not accurately reflect authorized configurations.

### Recommendation

We recommend that the FHFA Chief Information Officer:

22. Review and update the Common Control Plan, on a regular basis, to reflect which wireless networks are authorized to be set to broadcast.

[19] GAO-14-704G, *Standards for Internal Control in the Federal Government* (September 2014).

# FHFA COMMENTS AND OIG EVALUATION................................

We provided FHFA management an opportunity to review and provide technical comments on a draft of this audit report. We considered those comments in finalizing this report. In a written response, FHFA management agreed with our recommendations and included the following corrective actions, which we evaluated:

Recommendation 1

> OTIM has initiated a least privilege review and has begun to restrict access permissions on network drives. OTIM has also initiated an "Agency-wide" comprehensive folder review and update as needed to ensure the least privilege principle is enforced throughout the Agency. OTIM will complete the review and establish a protocol to ensure that folder access will comport with the least privilege principle by July 31, 2025.
>
> Management's planned corrective actions meet the intent of our recommendation.

Recommendation 2

> OTIM evaluated the need for the software script to generate and record user login records, determined that script generation is no longer required, and terminated the practice. Accordingly, OTIM also deleted the historical logs.
>
> Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 3

> On February 8, 2024, OTIM changed all remaining default or initial passwords to unique passwords. On May 21, 2024, OTIM validated that the default or initial login passwords were changed for all 179 users whose passwords were compromised in this audit.
>
> Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendations 4 and 5

> OTIM updated its password creation procedure on May 25, 2024. The new procedure requires FHFA's Help Desk or OTIM Operations staff to use a random password generator for all new accounts and for resetting passwords.
>
> Management's corrective actions, if implemented as stated, meet the intent of our recommendations.

Recommendation 6

As part of the onboarding process, OTIM will provide training to new employees and contractors on FHFA authentication and identification responsibilities. OTIM will semi-annually remind all employees and contractors of their FHFA authentication and identification responsibilities. The first notification occurred during annual security training on June 13, 2024, and the second notification will occur by December 31, 2024.

Management's corrective actions, planned or if already implemented as stated, meet the intent of our recommendation.

Recommendation 7

OTIM will evaluate all current methods used to access the FHFA network and ensure that each method uses multifactor authentication by December 31, 2024.

Management's planned corrective action meets the intent of our recommendation.

Recommendation 8

OTIM completed changes for the compromised cloud administrator account and documented the change on June 13, 2024.

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 9

OTIM will research an enterprise-wide solution for access to the Agency's cloud environment and use the research to create an implementation roadmap. If a solution cannot be implemented by March 30, 2025, OTIM will document and implement compensating controls.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 10

FHFA will contact its cloud providers to determine if multifactor authentication can be used to gain access to the cloud environment. If FHFA does not have a viable solution to enforce multifactor authentication to access its cloud environments, the Agency will develop compensating controls and document any risk-based decisions by March 30, 2025.

Management's planned corrective actions meet the intent of our recommendation.

Recommendations 11, 12, and 13

OTIM will assess current tools to determine if a data loss prevention (DLP) tool can be implemented by December 31, 2024. If a current tool cannot be used to implement a DLP solution, OTIM will research and make a decision to procure a DLP tool and create an implementation roadmap by July 30, 2025. FHFA notes that fully implementing a DLP solution will be a multiyear effort. FHFA will identify compensating controls or interim steps that can be implemented by July 30, 2025, to address the finding and related risk.

Management's planned corrective actions meet the intent of our recommendations.

Recommendation 14

OTIM will reevaluate the risk acceptance decision for portable software programs to determine if any changes are required by December 30, 2024. If changes are required, OTIM will procure and implement an application blocker.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 15

OTIM will assess current tools to determine if a tool to prevent unauthorized software downloads can be configured by October 31, 2024. If a current tool cannot be used to prevent unauthorized software downloads, OTIM will perform market research and identify an appropriate tool by July 31, 2025. FHFA notes that fully implementing an application with these capabilities will be a multiyear effort. FHFA will identify compensating controls or interim steps that can be implemented by July 31, 2025, to address the finding and related risk.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 16

OTIM will assess its current resources to determine if the Agency has the resources to comply with CISA BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022) by December 31, 2024. If OTIM determines that the Agency does not have the resources to comply with CISA BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022), OTIM will request and secure the additional resources to attain compliance by June 30, 2025.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 17

OTIM will develop a Plan of Action and Milestones to track the remediation of past due CISA Known Exploitable Vulnerabilities under CISA's BOD 22-01 and OTIM

Vulnerability Management Process, Revision 2.7 (September 7, 2022). OTIM will assess the feasibility of implementing compensating controls for each of the KEVs that cannot be remediated and perform a risk acceptance analysis by February 28, 2025.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 18

OTIM will prioritize existing resources based on the Plan of Action and Milestones to ensure that CISA Known Exploitable Vulnerabilities are remediated in accordance with CISA's BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022) by February 28, 2025.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 19

OTIM will reevaluate the former Chief Information Officer's risk acceptance related to the device lock policy and implement security controls to ensure that all FHFA laptops adhere to FHFA's device lock policy under FHFA System Security and Privacy Plan for the General Support System (June 5, 2023) by October 31, 2024.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 20

FHFA changed the policy to lock workstations when PIV cards are removed and distributed an Agency-wide notification on February 29, 2024. OTIM will remind employees and contractors semi-annually to securely lock their unattended devices. The first notification will occur by August 30, 2024.

Management's corrective actions, planned or if already implemented as stated, meet the intent of our recommendation.

Recommendation 21

OTIM currently employs a USB blocker. OTIM will conduct market research to identify a solution to block unauthorized devices from functioning when connected to USB ports and implement the solution by June 28, 2025.

Management's corrective actions, planned or if already implemented as stated, meet the intent of our recommendation.

Recommendation 22

OTIM will update the Common Control Plan to reflect which wireless networks may broadcast by September 30, 2024.

Management's planned corrective actions meet the intent of our recommendation.

Overall, we consider FHFA management responsive to the recommendations in this report. These recommendations will remain open until we confirm that corrective actions have been fully implemented. FHFA's written response, in its entirety, is included as Appendix II to this report.

# APPENDIX I: METHODOLOGY..............................................

To accomplish our objective, we performed the following procedures:

- Reviewed Government Accountability Office's *Standards for Internal Control in the Federal Government* (GAO-14-704G; September 2014) and determined that the design control activities component was significant to this objective. It focused on the underlying principle that: (1) general controls include physical access, (2) management evaluates security threats to information technology from internal and external sources, and (3) management designs controls over access to protect an entity from inappropriate access and unauthorized use.

- Reviewed the following NIST publications:

  - NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (updated December 2020)

  - NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* (September 30, 2008)

- Signed the Rules of Engagement with FHFA management that outlined the general parameters and period of our testing as well as protocols for reporting any successful intrusions,[20] which is a recommended practice by NIST. In line with the Rules of Engagement, we only attempted to exploit vulnerabilities during agreed upon test windows.

- Conducted an internal security assessment of FHFA's network and information systems in four phases: planning, discovery, attack, and reporting.

  - Planning phase: Identified rules, finalized and documented management approval, and set testing goals. This phase sets the groundwork for a successful test. No actual testing occurred in this phase.

  - Discovery phase: Gathered information from within FHFA's network and facilities to identify potential targets and obtain unprotected data about those targets. To find and map FHFA's systems, we used our licensed software to conduct automated scanning and standard operating system functions (e.g., ping, nslookup) to verify if

[20] An intrusion would have been considered successful if we had gained access to FHFA systems or data, which should have been denied. An intrusion would allow us to view or copy data, monitor user activities, install programs in memory, or otherwise control the target.

devices were active. We used a "white box" method, which is an assumption that we had knowledge of FHFA's network and systems prior to conducting our testing.

  - Vulnerability assessment phase: Checked FHFA's internal systems for known security vulnerabilities using automated commercial off-the-shelf software.

  - Exploitation phase: Used vulnerabilities discovered to gain unauthorized access to FHFA systems. An intrusion was deemed successful when access, which should have been denied, was gained, allowing OIG the ability to view or copy controlled data, monitor user activities, install programs in memory, or obtain full control over the target.

  - Reporting phase: Analyzed and compiled our test results and provided them to FHFA management. Met with FHFA staff and management to confirm reported vulnerabilities.

- Reviewed the following FHFA policies and procedures to determine FHFA's security controls and process for least privilege, authenticator management, information flow control, user-installed software, vulnerability management, device lock, and media use:

  - FHFA Access Control Standard, Revision 2.3 (November 30, 2022)

  - FHFA Common Control Plan, Revision 3.5 (May 10, 2023)

  - FHFA Information Systems Rules of Behavior and User Acknowledgement (December 2022)

  - FHFA System Security and Privacy Plan for the General Support System (June 5, 2023)

  - OTIM General Support System Information Security Architecture, Revision 2.5 (May 21, 2021)

  - OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022)

- Obtained and reviewed industry best practices for secure use of the cloud including CISA and NSA's *Use Secure Cloud Identity and Access Management Practices*, Ver. 1.0, (March 2024).

- Interviewed OTIM officials and staff regarding FHFA's implementation of security controls.

- Performed the following vulnerability and penetration tests:

    - Test 1: We used our OIG test laptops to discover and exploit vulnerabilities on FHFA's systems.  Using our FHFA network access, we connected our OIG test laptops to FHFA's network to perform network discovery and credential scanning of all systems connected to the internal network.  We ran tools to exploit any identified vulnerabilities to gain unauthorized access to FHFA's network and systems.  Our objective was to use our penetration test tools to discover and exploit vulnerabilities on FHFA's systems.

    - Test 2: We used our assigned laptop and FHFA standard user account as an insider to gain unauthorized access to FHFA's internal systems and information.  We used built-in operating system commands and tools to perform network discovery.  We used tools to gain unauthorized access to FHFA's internal systems, connect to unauthorized devices, alter configuration settings, and extract sensitive information. We elevated privileges to gain additional access to network resources and information.  Our objective was to gain access to all connected systems and files.

    - Test 3: We used FHFA's assigned PIV card to perform physical security testing of FHFA office space at headquarters.  Our objective was to gain unauthorized access to FHFA's network, systems, and information by circumventing FHFA's physical security controls and testing FHFA users' adherence to the FHFA Rules of Behavior.

- We conducted this performance audit between October 2023 and August 2024, at our headquarters in Washington, D.C., 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.

# APPENDIX II: FHFA MANAGEMENT RESPONSE.........................

This page intentionally blank.  See the following page(s).

**Federal Housing Finance Agency**

## MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audits

THROUGH: Mary Peterman, Acting Chief Operating Officer, OCOO

MARY PETERMAN

Digitally signed by MARY PETERMAN
Date: 2024.07.19 08:48:26 -04'00'

FROM: Luis Campudoni, Chief Information Officer

LUIS CAMPUDONI

Digitally signed by LUIS CAMPUDONI
Date: 2024.07.19 12:29:01 -04'00'

SUBJECT: Draft Audit Report: FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats

DATE: July 19, 2024

---

As FHFA's new Chief Information Officer, I appreciate the opportunity to review and respond to the above-referenced draft audit report (Report) by the Office of Inspector General (OIG), which contains 22 recommendations. This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the Report's 22 recommendations. I have tasked the Office of Technology and Information Management (OTIM) with developing and implementing a comprehensive plan to remediate the recommendations. I am committed to addressing the underlying Report findings, and OTIM has already initiated several remediation actions to address the recommendations.

***Recommendation 1:*** *Restrict user access to the folders and files on FHFA's network in accordance with least privilege principle.*

**Management Response for Recommendation 1:** FHFA agrees with the recommendation and has performed or will perform these actions:

1. OTIM has initiated a least privilege review and has begun to restrict access permissions on network drives.
2. OTIM has initiated an Agency-wide comprehensive folder review and update as needed to ensure the least privilege principle is enforced throughout the Agency. OTIM will complete the review and establish a protocol to ensure that folder access will comport with the least privilege principal by July 31, 2025.

***Recommendation 2:*** *Evaluate the need for the software script to generate and record user login records and restrict access to the log files in accordance with least privilege principle.*

**Management Response for Recommendation 2:** OTIM evaluated the need for the software script to generate and record user login records, determined that script generation is no longer required, and terminated the practice. Accordingly, OTIM also deleted the historical logs.

***Recommendation 3:*** *Ensure that the default or initial login passwords are changed for all 179 users whose passwords were compromised in this audit.*

**Management Response for Recommendation 3:** On February 8, 2024, OTIM changed all remaining default or initial passwords to a unique password. On May 21, 2024, OTIM validated that the default or initial login passwords were changed for all 179 users whose passwords were compromised in this audit.

***Recommendation 4:*** *Ensure that upon initial login, FHFA users establish a new password that meets FHFA requirements for length and complexity and that the password is not a commonly used or a known compromised password.*

***Recommendation 5:*** *Ensure that standard user accounts and privileged user accounts are not set up with the same default or initial login password.*

**Management Response for Recommendations 4 and 5:** On May 25, 2024, OTIM updated its password creation procedure. The new procedure requires FHFA's Help Desk or OTIM Operations staff to use a random password generator for all new accounts and for resetting passwords.

***Recommendation 6:*** *Ensure that personnel are trained on standard and privileged user FHFA authentication and identification policies.*

**Management Response for Recommendation 6:** FHFA agrees with Recommendation 6 and will perform these actions by December 31, 2024:

1. As part of the onboarding process, OTIM will provide training to new employees and contractors on FHFA authentication and identification responsibilities.
2. OTIM will semi-annually remind all employees and contractors of their FHFA authentication and identification responsibilities. The first notification occurred during annual security training that took place on June 13, 2024, and the second notification will occur by December 31, 2024.

***Recommendation 7:*** *Identify and implement a solution, in coordination with vendors, to ensure that multifactor authentication is required to access FHFA's network. If there are no viable solutions, document any risk-based decisions, including compensating controls.*

**Management Response for Recommendation 7:** FHFA agrees with Recommendation 7 and will evaluate all current methods used to access the FHFA network and ensure that each method uses multifactor authentication by December 31, 2024.

***Recommendation 8:*** *Change the credentials for the compromised cloud administrator account.*

**Management Response for Recommendation 8:** OTIM completed changes for the compromised cloud administrator account and documented the change on June 13, 2024.

***Recommendation 9:*** *Use the secure access method recommended by FHFA's cloud service provider to access the FHFA cloud environment.*

**Management Response for Recommendation 9:** FHFA agrees with Recommendation 9 and will complete these actions by March 30, 2025:

1. Perform research for an enterprise-wide solution on access to the Agency's cloud environment.
2. Use the research to create an implementation roadmap.
3. If a solution cannot be implemented by March 30, 2025, OTIM will document and implement compensating controls.

***Recommendation 10:*** *Identify and implement a solution, in coordination with vendors, to ensure multifactor authentication is required for privileged users to access FHFA's cloud environment. If there are no viable solutions, document any risk-based decisions, including compensating controls.*

**Management Response for Recommendation 10:** FHFA agrees with recommendation 10 and will perform these actions by March 30, 2025:

1. FHFA will contact its cloud providers to determine if multifactor authentication can be used to gain access to the cloud environment.
2. If FHFA does not have a viable solution to enforce multifactor authentication to access its cloud environments, the Agency will develop compensating controls and document any risk-based decisions.

***Recommendation 11:*** *Identify and implement a solution to detect and monitor the transfer of large amounts of data moving across FHFA's network.*

***Recommendation 12:*** *Identify and implement a solution to detect and prevent controlled unclassified information or personally identifiable information from being transferred outside of FHFA's network to personal accounts on email and cloud-based storage services.*

***Recommendation 13:*** *Determine whether resources can be made available to implement a data loss prevention system to prevent the exfiltration of controlled unclassified information.*

**Management Response for Recommendations 11, 12, and 13:** FHFA agrees with Recommendations 11, 12, and 13 and will perform these actions:

1. OTIM will assess current tools to determine if a data loss prevention tool (DLP) can be implemented by December 31, 2024.
2. If a current tool cannot be used to implement a DLP solution, OTIM will research and make a decision to procure a DLP tool and create an implementation roadmap by July 30, 2025.

FHFA notes that fully implementing a DLP solution will be a multiyear effort. FHFA will identify compensating controls and/or interim steps that can be implemented by July 30, 2025, to address the finding and related risk.

***Recommendation 14:*** *Reevaluate the former Acting Chief Information Officer's risk acceptance related to portable software programs, and implement security controls to detect and prevent users from downloading and running unapproved software on FHFA's system in accordance with NIST and FHFA's Rules of Behavior*.

**Management Response for Recommendation 14:** FHFA agrees with Recommendation 14 and will reevaluate the risk acceptance decision for portable software programs to determine if any changes are required by December 30, 2024. If changes are required, OTIM will procure and implement an application blocker.

***Recommendation 15:*** *Monitor and respond to unauthorized software downloads in accordance with FHFA's Common Control Plan.*

**Management Response for Recommendation 15:** FHFA agrees with Recommendation 15 and will perform these actions:

1. OTIM will assess current tools to determine if a tool to prevent unauthorized software downloads can be configured by October 31, 2024.
2. If a current tool cannot be used to prevent unauthorized software downloads, OTIM will perform market research and identify an appropriate tool by July 31, 2025.

FHFA notes that fully implementing an application with these capabilities will be a multiyear effort. FHFA will identify compensating controls and/or interim steps that can be implemented by July 31, 2025, to address the finding and related risk.

***Recommendation 16:*** *Identify and secure the resources necessary to remediate identified internal critical, high, and medium exploitable vulnerabilities on the FHFA servers, workstations, and other devices in compliance with CISA BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022).*

**Management Response for Recommendation 16:** FHFA agrees with recommendation 16 and will perform these actions:

1. OTIM will assess its current resources to determine if the Agency has the resources to comply with CISA BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022) by December 31, 2024.
2. If OTIM determines that the Agency does not have the resources to comply with CISA BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022), OTIM will request and secure the additional resources to attain compliance by June 30, 2025.

***Recommendation 17:*** *Develop a Plan of Action and Milestones to track the remediation of past due CISA Known Exploitable Vulnerabilities in accordance with CISA's BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022). OTIM should implement compensating controls (i.e., isolating systems with un-remediated vulnerabilities) to mitigate the risk of the vulnerabilities.*

**Management Response for Recommendation 17:** FHFA agrees with recommendation 17 and will perform these actions by February 28, 2025:

1. OTIM will develop a Plan of Action and Milestones to track the remediation of past due CISA Known Exploitable Vulnerabilities (KEV) under CISA's BOD 22-01 and OTIM *Vulnerability Management Process*, Revision 2.7 (September 7, 2022).
2. OTIM will assess the feasibility of implementing compensating controls for each of the KEVs that cannot be remediated and perform a risk acceptance analysis by February 28, 2025.

***Recommendation 18:*** *Prioritize existing OTIM resources based on the Plan of Action and Milestones to ensure that CISA Known Exploitable Vulnerabilities are remediated in accordance with CISA's BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022).*

**Management Response for Recommendation 18:** FHFA agrees with Recommendation 18 and will prioritize existing OTIM resources based on the Plan of Action and Milestones to ensure that CISA Known Exploitable Vulnerabilities are remediated in accordance with

CISA's BOD 22-01 and OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022) by February 28, 2025.

***Recommendation 19:*** *Reevaluate the former Chief Information Officer's risk acceptance related to the device lock policy and implement security controls to ensure that all FHFA laptops adhere to FHFA's device lock policy in accordance with FHFA System Security and Privacy Plan for the General Support System (June 5, 2023).*

**Management Response for Recommendation 19:** FHFA agrees with Recommendation 19 and will reevaluate the former Chief Information Officer's risk acceptance related to the device lock policy and implement security controls to ensure that all FHFA laptops adhere to FHFA's device lock policy under FHFA *System Security and Privacy Plan for the General Support System* (June 5, 2023) by October 31, 2024.

***Recommendation 20:*** *Emphasize through training an FHFA user's responsibility to securely lock their unattended devices.*

**Management Response for Recommendation 20:** FHFA agrees with Recommendation 20 and has performed or will perform these tasks.

1. FHFA changed the policy to lock workstations when PIV cards are removed and distributed an Agency-wide notification on February 29, 2024.
2. OTIM will remind employees and contractors semi-annually to securely lock their unattended devices. The first notification will occur by August 30, 2024.

***Recommendation 21:*** *Implement security controls to lock down USB ports so that only authorized USB devices are allowed.*

**Management Response for Recommendation 21:** FHFA agrees with Recommendation 21 and has performed or will perform these actions by June 28, 2025:

1. OTIM currently employs a USB blocker.
2. OTIM will conduct market research to identify a solution to block unauthorized devices from functioning when connected to USB ports and implement the solution.

***Recommendation 22:*** *Review and update the Common Control Plan, on a regular basis, to reflect which wireless networks are authorized to be set to broadcast.*

**Management Response for Recommendation 22:** FHFA agrees with Recommendation 22 and will update the Common Control Plan to reflect which wireless networks may broadcast by September 30, 2024.

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
John Major
Warren Hammond
Stuart Levy
Ralph Mosios

Federal Housing Finance Agency
Office of Inspector General

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