REDACTED

Federal Housing Finance Agency
Office of Inspector General

2019 Internal Penetration Test of FHFA's Network and Systems

This report contains redactions of information that is privileged or confidential.

Audit Report • AUD-2019-014 • September 24, 2019

AUD-2019-014

September 24, 2019

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, Freddie Mac, and the Federal Home Loan Bank System. Within FHFA, the Office of Technology and Information Management (OTIM) works with the Agency's offices to promote the effective and secure use of information and systems.

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. FISMA also requires inspectors general to perform annual independent evaluations of their respective agencies' information security program and practices. The annual FISMA audit of FHFA, however, does not include penetration testing of FHFA's network and systems. In 2018, we performed an external penetration test of FHFA's network and systems. This year, we performed an internal penetration test to determine whether FHFA's security controls were effective to protect its network and systems against internal threats. For purposes of this audit, we were given the same access a typical FHFA employee would be given—general user access with no special rights or privileges.

Using the access given to a typical FHFA employee, we determined that FHFA's network, systems, and information were not sufficiently protected against insider threats. We found:

- an FHFA wireless network intended for employees' personal use of the internet improperly allowed non-FHFA-issued devices to access FHFA's internal network. Through this wireless network connection, we were able to scan FHFA servers. Our scanning tools identified high severity and medium severity vulnerabilities related to outdated [redacted] and [redacted] protocols in FHFA's systems.

- sensitive information [redacted] We also demonstrated to FHFA our capability to [redacted] this information.

- some offices in FHFA's headquarters building were open outside of business hours with sensitive information left unattended and plainly visible. We were also able to access sensitive information by [redacted] located in some of those offices.

- controls did not prevent the use of unapproved programs [redacted] (known as “[redacted]”).
- default administrator passwords were not changed on [redacted].

As these control deficiencies were identified during our audit, we brought them to the attention of FHFA management who took or began to take remedial actions to address them. These vulnerabilities, if not remediated, pose risk to FHFA’s network, systems, and information. Continued management attention and action is required to ensure that FHFA’s security controls protect its network and systems against internal threats.

We make six recommendations in this report. In a written management response, FHFA agreed with our recommendations.

This report was prepared by Jackie Dang, IT Audit Director; Dan Jensen, Auditor-in-Charge; and Nick Peppers, IT Specialist; with assistance from 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.

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, Deputy Inspector General for Audits /s/

TABLE OF CONTENTS ....

ABBREVIATIONS

CVSS	Common Vulnerability Scoring System
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
IT	Information Technology
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
NIST SP 800-53	NIST Special Publication, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
OTIM	Office of Technology and Information Management
PII	Personally Identifiable Information
PIV	Personal Identity Verification
SP	Special Publication
[redacted]	[redacted]

BACKGROUND

Standards for Information Security Controls and Testing

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) is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.

For FHFA, the FISMA-required annual independent evaluations are performed by an independent external auditor under contract with our office. For fiscal year 2018,[1] the audit found that FHFA complied with FISMA and related Office of Management and Budget guidance, and that sampled security controls selected from NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53), demonstrated operating effectiveness.[2]

NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, provides guidelines for designing, implementing, and maintaining technical information relating to security testing. It describes several techniques for identifying targets and analyzing them for potential vulnerabilities, such as network discovery, network port and service identification, vulnerability scanning, and wireless scanning. According to NIST, testing for vulnerabilities also includes non-technical methods such as physical security testing. Physical security testing includes attempts to circumvent locks, badge readers, and other physical security controls. By circumventing physical controls, testers have additional methods available to access networks, equipment, and sensitive information [redacted][3]

[1] As of the date of this report, our FISMA audit of FHFA for fiscal year 2019 is under way.

[2] NIST SP 800-53 provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats, including hostile cyberattacks, natural disasters, structural failures, and human errors.

[3] [redacted]

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 (PII)[4] of employees. FISMA requires FHFA to ensure controls are implemented to safeguard its information from unauthorized access and manipulation.

Before FHFA network users (i.e., employees, interns, and contractors) are given access to the FHFA network, they must agree to the FHFA “Rules of Behavior.” The Rules of Behavior describe what the user is permitted to do, their responsibilities, and certain prohibited activities (e.g., attaching unauthorized devices to the network, installing unauthorized software, circumventing management controls, etc.). Acknowledging the Rules of Behavior agreement is an annual requirement of all users to maintain access to FHFA’s network and systems.

Each FHFA user also receives annual training on information security awareness, including topics such as information security tips, password help, and whom to contact in the event of a security breach. Furthermore, those users with significant information security roles receive additional training. This advanced, “role-based” training is intended to ensure that those people with increased access and responsibility are trained on topics like protection of PII and breach mitigation procedures.

* * * * *

Because the annual FISMA audit does not include penetration testing of systems or network security, we undertook this audit to determine whether FHFA’s security controls were effective to protect its network and systems against internal threats. For purposes of this audit, we had the access given to a typical FHFA employee with no special rights or privileges – an employee with general user access.

Consistent with NIST guidance, we established, with FHFA management, Rules of Engagement before we began work on this audit. The Rules of Engagement were agreed upon and signed by the Chief Information Officer for FHFA and the Deputy Inspector General for Audits for OIG. 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 penetration testing. However, as stated in the Rules of Engagement, the

[4] PII is defined by the Office of Management and Budget as information that can be used to distinguish or trace an individual’s identity, and can include a person’s name, social security number, date and place of birth, and financial and employment information.

document does not limit the authority of OIG to conduct audits in accordance with the Inspector General Act of 1978, as amended.

FACTS AND ANALYSIS ....

One method to test the adequacy of a system's internal controls is penetration testing. See NIST SP 800-53. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can include testing of both physical and technical security controls. Penetration testing also includes non-technical methods of attack: it attempts to breach physical security controls and procedures to connect to a network, steal equipment, or capture sensitive information (such as [redacted]).

Penetration testing can be conducted from inside or outside an organization's security perimeter. For purposes of this audit, we conducted inside penetration testing to identify possible vulnerabilities that could be exploited by an "insider threat." An insider threat is someone who has some level of access to the organization and, intentionally or not, can gain or provide access to sensitive information. Insider threats can be attackers who have penetrated the first line of network defenses, malicious employees intending to harm the organization or profit from exposing sensitive information, or unwitting employees who enable others to access the network through careless behavior.

Internal Vulnerability Testing Found that an FHFA Wireless Network Intended Only for Personal Use by Employees Improperly Allowed Non-FHFA-Issued Devices to Access FHFA's Internal Network

FHFA provides its employees access to a wireless network called "[redacted]" to access the internet with their personally owned devices (e.g., mobile phones, tablets, etc.; devices not issued by FHFA). In internal vulnerability testing, we found that, through the [redacted], we could connect an OIG laptop (i.e., a non-FHFA-issued device) not just to the internet but also to FHFA's internal network.[5]

Once connected to FHFA's internal network through the [redacted], we continued our internal vulnerability testing to assess what a malicious insider might do. We conducted a scan of FHFA's servers with a [redacted]

[5] FHFA policies prohibit users from attaching any unauthorized computing device to the FHFA network.

[redacted] that we [redacted].[6] With this tool, we were able to scan 23 FHFA servers, without detection by FHFA's network monitoring tools. Near the end of the testing window, we connected a second OIG laptop to FHFA's internal network, again through [redacted], and conducted a [redacted] scan of FHFA's network using a different [redacted] This [redacted] scan was detected by FHFA's network monitoring tool, which sent out an alert to OTIM's staff during the night, and they disconnected our second laptop's connection to [redacted] the next morning resulting in termination of our scan. However, before termination, our tool had completed scans of 145 FHFA systems.

OTIM reported that it reconfigured [redacted] to prevent access to FHFA's internal network. Our subsequent testing found that this remedial action prevented further access to FHFA's internal network through [redacted].

Our Scanning Tools Identified High Severity and Medium Severity Vulnerabilities in FHFA's Systems, But We Were Unable to Exploit Them

Our scans, performed with OIG laptops connected to the FHFA internal network through [redacted], identified high- and medium-severity vulnerabilities[7] related to an outdated [redacted] protocol[8] and an outdated [redacted] protocol.[9] We did not attempt to exploit these vulnerabilities.

We provided the results of our vulnerability scanning to FHFA management during fieldwork. FHFA management told us that the outdated [redacted] protocol was disabled for FHFA's public-facing servers in response to a recommendation from our external penetration test report conducted earlier this year, but the outdated [redacted] protocol had not been

[6] 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.

[7] 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.

[8] [redacted]

[9] [redacted]

disabled for the [redacted].[10] With respect to the outdated [redacted] protocol, management reported that after receiving the results of our tests they disabled it.

Internal Penetration Testing Found that Sensitive Information [redacted]

NIST requires that organizations only allow access necessary to accomplish assigned tasks in accordance with missions and business functions – the "least privilege" principle.[11] Using our assigned FHFA computer and our access rights as an FHFA employee (provided solely for this testing), we were able to access [redacted] in apparent contravention to the least privilege principle. Some of the files we accessed included [redacted] The open availability of these [redacted] could pose risks of [redacted]

[redacted] [12] [redacted] Among other things, [redacted] We were able to [redacted], because we agreed not to, we demonstrated our capability to do so to an OTIM official.

[10] *See* OIG, *External Penetration Test of FHFA's Network and Systems During 2018* (Feb. 11, 2019) (AUD-2019-003) (available online ***here***).

[11] NIST SP 800-53, Rev. 4., *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).

[12] [redacted]

Physical Security Controls Within FHFA's Headquarters Building Did Not Prevent Access to the Offices and Information of [redacted] and Other FHFA Employees

As discussed above, the vulnerability testing we conducted included physical security testing to assess the adequacy of physical security controls, such as locks, badge readers, and other controls. FHFA's Rules of Behavior prescribe users' responsibility to protect FHFA information systems and information from loss or compromise, including not writing passwords on visibly observable media such as sticky notes.

Our physical security testing at FHFA's headquarters building found the following:

Sensitive Information Unattended and Plainly Visible

We observed that some office doors of [redacted] and other FHFA employees were left open and/or unlocked before and after core business hours. Specifically, we observed from the opened door of [redacted], a Personal Identity Verification (PIV) card sticking out from under the keyboard on the [redacted]. When we entered the opened office door and lifted the keyboard, we also saw a temporary identification badge and a building access card. According to NIST SP 800-53, these type of access cards must be secured. In another instance, from the opened door of an [redacted], we observed a bright orange Universal Serial Bus storage device taped to a folded piece of paper, reading "[redacted] Server Encryption Keys Backup Copy," on the [redacted]. The device, if labeled correctly, may have contained encryption keys for [redacted] When we went into offices with opened doors, we also observed sensitive items were in plain sight, including:

- A sticky note on which a Personal Identification Number (PIN) for a [redacted] iPad was written;
- Network sensitive information that included schedules of network scans and internet protocol addresses; and
- A list of visitors who are exempt from building security screening.

The lack of security for this sensitive information made it accessible to users who were not otherwise authorized to access it.

Unattended Access to Desktop Computers

For three of the offices where we found open doors outside of business hours, we sought to access sensitive information on the unattended computers [redacted]. [redacted]

[redacted]. More than a day later, [redacted]

[redacted].

[redacted]

Controls Did Not Prevent the Use of Unauthorized Programs

FHFA policies prohibit users from installing unauthorized programs on FHFA computers. We found that FHFA computers included a technical control designed to prevent users from installing programs. FHFA policy also states that all programs not on its approved software list are considered unauthorized.[13] FHFA's Rules of Behavior, to which each FHFA network user must agree, directs: "Do not alter the configuration of any FHFA computing device, or override, defeat, or circumvent any security, technical, or management controls employed by the Agency."

[13] The approved software list is a management control employed by the Agency.

Using our assigned FHFA laptop, we tested whether an FHFA user could download, install,[14] and run unapproved programs and were not able to do so. However, we were able to [redacted][15] For example, we were able to [redacted], circumventing a management control in violation of the Rules of Behavior. After we brought this to management's attention, we were informed that FHFA is establishing a process for detecting and responding to the use of [redacted].

[redacted] Had Default Administrator Passwords

[redacted] We tested three [redacted] that we were told were representative of the [redacted]. Our testing found that all three of the [redacted] that we tested still had the default passwords in effect for administrator accounts;[16] those default passwords were [redacted]. The administrator account is used to manage the accounts and [redacted]. With knowledge of the default password, a malicious insider [redacted] the information. We did not attempt to exploit this potential vulnerability using these default passwords. After we briefed management on this issue, we were informed that the administrator passwords were changed for all [redacted]. However, our testing of this remedial measure on one [redacted] found that the default administrator password had not been changed.

FINDINGS ....

[redacted] Allowed Non-FHFA-Issued Devices to Access FHFA's Internal Network

FHFA policies prohibit users from attaching any unauthorized computing device to the FHFA network. Through [redacted], a wireless network providing employees access to the

[14] Installation is the process of creating, extracting, and moving the necessary files to run a program on a computer. This is typically done by downloading an installer program and running it on a computer, which also typically requires administrative privileges.

[15] [redacted]

[16] NIST requires that default passwords be changed before assets are deployed.

[17] NIST defines [redacted]

internet with their personally owned devices, we were able to connect a non-FHFA-issued device to FHFA's internal network and run scans to search for vulnerabilities. During our audit, OTIM reported that it reconfigured [redacted] to prevent access to FHFA's internal network. Our subsequent testing found that this remedial action did prevent us from accessing FHFA's internal network through [redacted]. Consistent with FISMA guidance, periodic tests should be performed to ensure such wireless networks do not improperly allow access to FHFA's internal network.

Outdated Security Protocols Were in Use

Our scans of FHFA's internal network identified vulnerabilities related to an outdated [redacted] protocol and an outdated [redacted] protocol, in apparent contravention to NIST directives. Allowing outdated protocols such as the ones we found could jeopardize the confidentiality of information on the FHFA network, allowing an insider threat to eavesdrop on network connections more easily. During our audit, FHFA management provided evidence that these outdated protocols were disabled.

Sensitive Information on [redacted] Was Available to [redacted]

NIST directs organizations to limit information access to those who have a genuine need for that information in the scope of their professional duties (i.e., the least privilege principle). We found that [redacted] in apparent contravention to the least privilege principle. Among these [redacted] The open availability of these [redacted] could pose risks of [redacted]

Some Employees Did Not Adhere to Physical Security Requirements Designed to Protect Sensitive Information

FHFA's Rules of Behavior requires users to protect FHFA information systems and information from loss or compromise. When we walked through the FHFA headquarters building outside of business hours, we observed a number of offices with their doors left open. Inside several of those offices, we observed documents left on top of desks containing sensitive information and passwords. We were also able to [redacted] in some of those offices, which allowed us [redacted].

Unauthorized Programs Could Be [redacted] on FHFA Computers

FHFA policies prohibit users from installing unauthorized programs on FHFA computers. We found that FHFA computers included a technical control that prevented users from downloading, installing, and running unapproved programs. However, we were able to [redacted] circumvent other FHFA controls in violation of FHFA's Rules of Behavior, [redacted]. Management reported that they are establishing a process for detecting and responding to the use of [redacted].

Default Administrator Passwords Were in Use on [redacted]

NIST requires that default passwords be changed before assets are deployed. We found that the default administrator password for all three sampled [redacted] we tested had not been changed. After bringing this control weakness to management's attention, we were informed that the passwords were changed for all [redacted]. However, our subsequent testing of this remedial measure on one [redacted] found that the default password had not been changed. Default administrator passwords could allow unauthorized use of an [redacted] sensitive information.

CONCLUSION...

Our internal penetration tests found certain FHFA security controls worked as intended, but others did not. Without detection, we were able to access FHFA's internal network with non-FHFA-issued computers and with that access we were able to run scans of many servers on FHFA's network to search for vulnerabilities. Those scans identified outdated security protocols (which we did not attempt to exploit). We also found that [redacted] sensitive information on [redacted] which also could have been [redacted] Employee adherence to physical security over information and computer assets was also problematic; we were able to view sensitive information on [redacted] outside of business hours because their office doors were open and the information was not otherwise secured. Furthermore, we were able to collect sensitive information by [redacted] in some of those offices. While FHFA's technical controls prevented the installation of unapproved programs on FHFA computers, [redacted] Lastly, we found default administrator passwords were not changed on all [redacted], a weakness that could allow the [redacted] of sensitive information.

Consistent with the Rules of Engagement, we brought these weaknesses to management's attention during our audit, and management either took or initiated remedial action for most weaknesses. However, our subsequent testing of one remedial action – the changing of default administrator passwords on [redacted] – found it was not effective. In summary, continued management attention and action is required to ensure that FHFA's security controls protect its network and systems against internal threats.

RECOMMENDATIONS...

We recommend that FHFA:

1. Perform tests periodically, and take action as appropriate, to ensure non-FHFA-issued devices cannot connect to the FHFA internal network through [redacted] or similar wireless networks made available to employees for their personal devices.

2. Ensure that outdated [redacted] and [redacted] protocols in FHFA's systems are disabled or upgraded in a timely manner in accordance with NIST directives.

3. Restrict user access to [redacted] in accordance with the least privilege principle.

4. Emphasize through training and enforcement employees' responsibilities to secure sensitive information. Consider including information in training about the means, such as [redacted], malicious insiders may use to obtain access to sensitive information.

5. Implement controls to prevent users from running unapproved [redacted] on FHFA's systems.

6. Change default administrative passwords for all existing [redacted], and implement a control to ensure that default administrative passwords are changed before such devices are deployed and placed in service.

FHFA COMMENTS AND OIG RESPONSE..................................

We provided FHFA an opportunity to respond to a draft of this audit report. In its management response, which is included in the Appendix to this report, FHFA agreed with all six of our recommendations and included the following completed and planned corrective actions:

1. OTIM modified the [redacted] access control list in June 2019 to ensure that FHFA's internal network could not be accessed from [redacted]. The General Support System's Owner will review the [redacted] access control list annually, and OTIM will review and approve future [redacted] access control list changes prior to implementation. This process will be completed by August 31, 2020.

2. OTIM will scan or review [redacted] and [redacted] protocols used by FHFA to ensure they comply with NIST directives by August 31, 2020.

3. FHFA will educate and remind information owners to annually review and, if necessary, update permissions for compliance with the least privilege principle by August 31, 2020.

4. FHFA will add the Controlled Unclassified Information procedures and workspace impact training to the new employee orientation by November 30, 2019, annually or more frequently remind employees and contractors about securing their workspace per the Controlled Unclassified Information procedures and training by September 30, 2019, and add insider threat information to its Information Security training by August 31, 2019.

5. FHFA will conduct a feasibility analysis of implementing an application blocker for [redacted] by August 31, 2020, review and modify as necessary its approved software standard by August 31, 2020, and annually remind employees that downloading unapproved software violates the Agency's Rules of Behavior by August 31, 2020.

6. FHFA will validate that all [redacted] default passwords have been changed by November 30, 2019, and update its procedures to ensure that [redacted] default passwords are changed prior to installing new devices on the FHFA network by August 31, 2020.

We consider FHFA's completed and planned corrective actions responsive to our recommendations. For Recommendation 3, we noted that management's estimated target date for implementation is August 31, 2020; given the nature of the sensitive information on the [redacted], we encourage management to complete its planned actions as expeditiously as possible.

OBJECTIVE, SCOPE, AND METHODOLOGY ....

The objective of this audit was to determine whether FHFA's security controls were effective to protect its network and systems against internal threats. Specifically, we performed an internal penetration test on FHFA's network and systems that can be accessed from an employee workstation, which included (but was not limited to) attempting to access internal connections and wireless connections accessible from within FHFA's physically secured space, examining logs and monitoring procedures, and evaluating related mitigating controls.

We undertook this audit to help FHFA protect itself and its employees from insider threats, such as a malicious employee with access to FHFA's network. As is a recommended practice by NIST, we established Rules of Engagement with FHFA management before we began work on this assignment. Among other things, the Rules of Engagement outlined the parameters and period of our testing as well as the protocols for reporting any successful intrusions. It also gave us authority to conduct defined activities without the need for additional permissions. The Rules of Engagement for this audit were agreed upon and signed by the Chief Information Officer for FHFA and the Deputy Inspector General for Audits for OIG. The period of our testing window on FHFA's network and systems for this audit, pursuant to the Rules of Engagement, was February 27, 2019, through April 26, 2019.

In performing this audit, a limited number of key FHFA managers were aware of it and provided us with access to accounts typical of FHFA's general users and with FHFA laptop computers typical of those issued to all FHFA employees; we were given no special privileges. We used the resources provided and [redacted] in tandem with built-in operating system functions and commands to gather information about FHFA's internal network systems and assets, to identify systems and data likely to be of interest to an attacker, and to test specific vulnerabilities in those systems. We also performed several tests of FHFA's wireless networks inside FHFA's headquarters building.

We conducted our internal penetration tests of FHFA's information systems in four phases: discovery, vulnerability assessment, exploitation, and reporting.

- Discovery – We 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 standard operating system functions ([redacted] [redacted][18]) to identify systems of interest and then used our [redacted] to conduct scanning and manually verify specific situations.

- Vulnerability Assessment – We focused on checking FHFA's internal systems for [redacted] security vulnerabilities.

[18] [redacted]

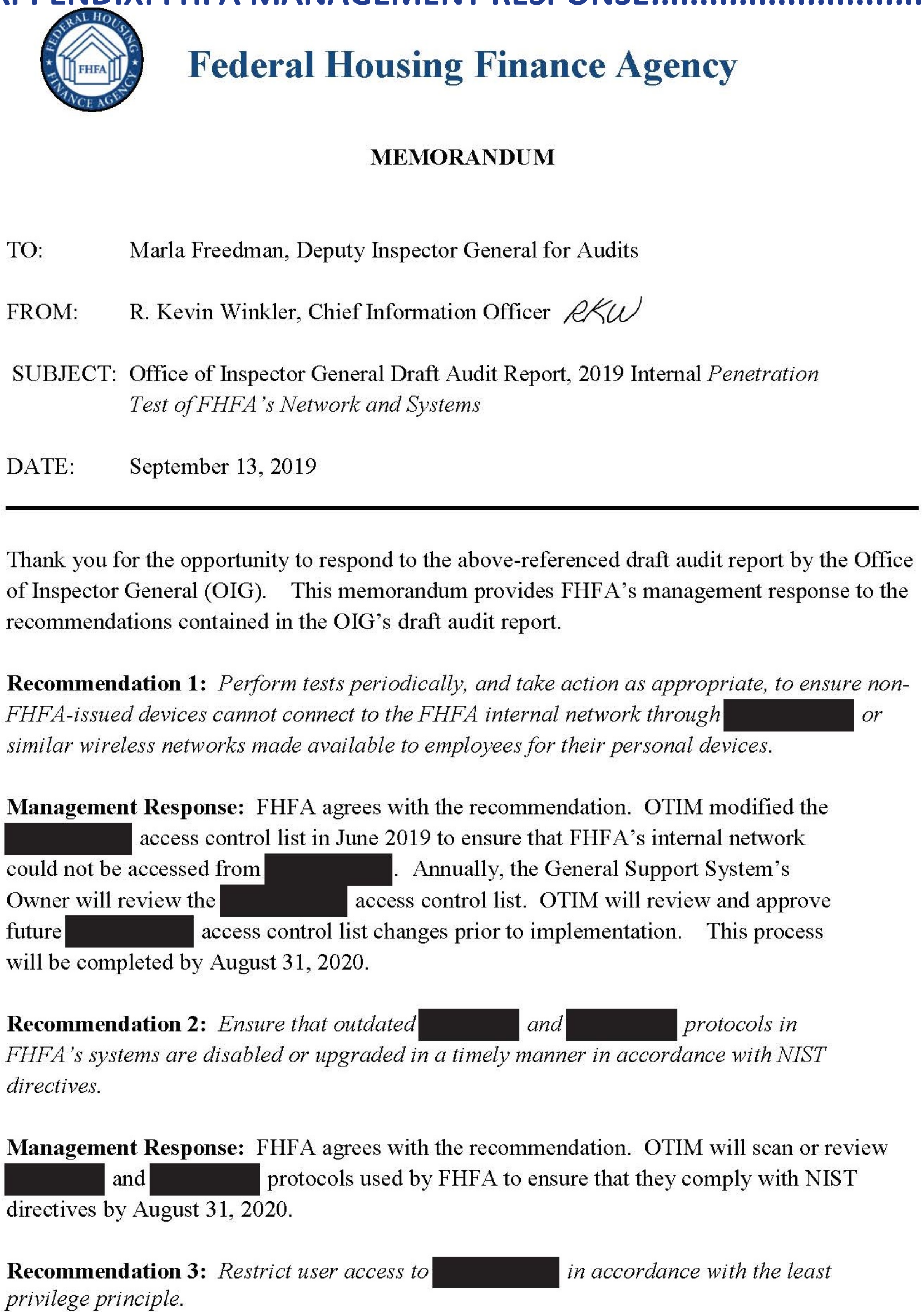
- Exploitation – We attempted to gain unauthorized increased access to FHFA systems using the vulnerabilities discovered.

- Reporting – We analyzed and compiled our test results then provided them to Agency management for review. We then met with FHFA management to confirm reported vulnerabilities and false positives. We did not include false positives in our report.

An exploitation was considered successful if we gained access to FHFA systems or data, where we should have been denied, and allowed us the ability to view/copy data, monitor user activities, install programs in memory, or otherwise control the target of our exploitation.

We conducted this performance audit between December 2018 and September 2019 in accordance with generally accepted government auditing standards. Those standards require that audits be planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our conclusions, based on our audit objective.

APPENDIX: FHFA MANAGEMENT RESPONSE...........................



Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Deputy Inspector General for Audits

FROM: R. Kevin Winkler, Chief Information Officer RKW

SUBJECT: Office of Inspector General Draft Audit Report, 2019 Internal *Penetration Test of FHFA's Network and Systems*

DATE: September 13, 2019

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

Recommendation 1: *Perform tests periodically, and take action as appropriate, to ensure non-FHFA-issued devices cannot connect to the FHFA internal network through* [redacted] *or similar wireless networks made available to employees for their personal devices.*

Management Response: FHFA agrees with the recommendation. OTIM modified the [redacted] access control list in June 2019 to ensure that FHFA's internal network could not be accessed from [redacted]. Annually, the General Support System's Owner will review the [redacted] access control list. OTIM will review and approve future [redacted] access control list changes prior to implementation. This process will be completed by August 31, 2020.

Recommendation 2: *Ensure that outdated* [redacted] *and* [redacted] *protocols in FHFA's systems are disabled or upgraded in a timely manner in accordance with NIST directives.*

Management Response: FHFA agrees with the recommendation. OTIM will scan or review [redacted] and [redacted] protocols used by FHFA to ensure that they comply with NIST directives by August 31, 2020.

Recommendation 3: *Restrict user access to* [redacted] *in accordance with the least privilege principle.*

Management Response: FHFA agrees with the recommendation and will take the following action:

a) FHFA will educate and remind information owners to annually review and if necessary, update permissions for compliance with the least privilege principle by August 31, 2020.

Recommendation 4: *Emphasize through training and enforcement employees' responsibilities to secure sensitive information. Consider including information in training about the means, such as* [redacted]*, malicious insiders may use to obtain access to sensitive information.*

Management Response: FHFA agrees with the recommendation and will take the following actions:

a) FHFA will add the Controlled Unclassified Information (CUI) procedures and workspace impact training to the new employee orientation by November 30, 2019;

b) FHFA will annually or more frequently remind employees and contractors about securing their workspace, per the CUI procedures and training by September 30, 2019; and

c) FHFA will add insider threat information to its Information Security training by August 31, 2020.

Recommendation 5: *Implement controls to prevent users from running unapproved* [redacted] *on FHFA's systems.*

Management Response: FHFA agrees with the recommendation and will take the following actions:

a) FHFA will conduct a feasibility analysis of implementing an application blocker for [redacted] by August 31, 2020;

b) FHFA will review and modify as necessary its approved software standard by August 31, 2020; and

c) FHFA will annually remind employees that downloading unapproved software violates the Agency's Rules of Behavior by August 31, 2020.

Recommendation 6: *Change default administrative passwords for all existing* [redacted]*s, and implement a control to ensure that default administrative passwords are changed before such devices are deployed and placed in service.*

Management Response: FHFA agrees with the recommendation and will take the following actions:

a) FHFA will validate that all [redacted] default passwords have been changed by November 30, 2019; and

b) FHFA will update its procedures to ensure that [redacted]' default passwords are changed prior to installing new devices on the FHFA network, by August 31, 2020.

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

CC: Chris Bosland
Larry Stauffer
T. Leach
J. Major
R. Mosios
C. Sherman
J. Vercellone
E. Hall
D. Crites
S. Levy

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