REDACTED

Federal Housing Finance Agency
Office of Inspector General

External Penetration Test of FHFA's Network and Systems During 2018

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

Audit Report • AUD-2019-003 • February 11, 2019

AUD-2019-003

February 11, 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) manages FHFA's information technology (IT) resources, including internet connections and internet accessible computers. 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, and to periodically test those assets. To support our ongoing oversight of FHFA's implementation of FISMA, we perform audits of networks and information security of the Agency. In this audit, we sought to determine whether FHFA's security controls were effective to protect its network and systems against external threats.

We found that FHFA's security controls successfully prevented us from gaining unauthorized access to its systems via the internet, wireless access points, or phishing email. Through a vulnerability scan of the Internet Protocol (IP) addresses registered to FHFA, we identified two medium severity vulnerabilities related to an outdated encryption protocol and web cookies; however, we were not able to exploit these vulnerabilities to gain unauthorized access to FHFA's systems. Upon receiving our vulnerability scan reports, FHFA management reported that a plan is underway to replace systems with an outdated encryption protocol and FHFA took action to address the web cookie vulnerability. We also performed an email phishing test that resulted in some users [redacted] in our phishing email.

We make three recommendations in this report. In a written management response, FHFA agreed with our recommendations. FHFA's reportedly completed and planned corrective actions are responsive to 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, 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 (OMB), and others, and will be posted on our website, www.fhfaoig.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
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OTIM	Office of Technology and Information Management
SP	Special Publication
[redacted]	[redacted]

BACKGROUND

FHFA was created by Congress in 2008 and is charged by the Housing and Economic Recovery Act of 2008 with oversight of the two housing-related government sponsored enterprises, Fannie Mae and Freddie Mac, and the Federal Home Loan Bank System. Since September 2008, FHFA has also served as the conservator of Fannie Mae and Freddie Mac. FHFA's mission is to ensure that these regulated entities operate in a safe and sound manner so that they serve as a reliable source of liquidity and funding for housing finance and community investment.

FHFA's OTIM works with all mission and support offices to promote the effective and secure use of information and systems. OTIM's goals are to: contribute to FHFA's mission by ensuring the availability of critical computer systems to FHFA staff; effectively and efficiently manage FHFA's technology resources and investments; identify technologies and tools to increase the productivity and efficiency of FHFA staff; ensure the security of FHFA information and systems; and develop strategic plans and goals for using advances in data and technology.

FISMA requires agencies, including FHFA, to develop, document, and implement agency-wide programs to provide information security for the information and information systems that support the operations and assets of the agency. In addition, FISMA requires agencies to implement periodic testing and evaluation of the effectiveness of security policies, procedures, and practices. Pursuant to FISMA, the National Institute of Standards and Technology (NIST) prescribes standards and guidelines pertaining to Federal information systems. The standards prescribed include information security standards that provide minimum information security requirements necessary to improve the security of Federal information and information systems. In addition, NIST develops and issues Special Publications (SP) as recommendations and guidance documents.

FISMA also requires Inspectors General to perform annual independent evaluations of their respective agencies' information security program and practices to determine the effectiveness of that program and practices. For FHFA, these annual independent evaluations are performed by an independent external auditor under contract with the Office of Inspector General. For fiscal year 2017, based on its audit work, the auditor determined that FHFA complied with FISMA and related OMB guidance, and that sampled security controls selected from NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, demonstrated operating effectiveness.

NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, provides guidelines for organizations on planning and conducting technical information security testing

and assessments, analyzing findings, and developing mitigation strategies. It provides practical recommendations for designing, implementing, and maintaining technical information relating to security testing and assessment processes and procedures, which can be used for several purposes—such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements.

External security testing is conducted from outside the organization's security perimeter. Such testing offers the ability to view the organization's security posture as it appears outside the security perimeter—usually as seen from the internet—with the goal of revealing vulnerabilities that could be exploited by external attackers.

FHFA's Network and Systems

FHFA's network and systems process and host FHFA data and information such as financial reports, loan data from the Enterprises, and examinations and analyses of the regulated entities. FISMA requires FHFA to ensure controls are implemented to safeguard its information from unauthorized access and manipulation. Networks and systems connected to the internet provide access points and therefore pose unique risks to the Agency in safeguarding its information. FHFA has implemented a security program that includes security testing and assessments for determining how effective the security controls implemented for the Agency's information systems are in safeguarding its nonpublic information. Information security testing both identifies vulnerabilities that can be exploited and assesses risk to an organization's IT systems. A security assessment includes gathering information to assist in developing the assessment approach, identifying and validating vulnerabilities, analyzing those vulnerabilities to identify root causes, and establishing mitigation strategies. A security assessment may include a variety of techniques, including, for example, vulnerability scanning, wireless scanning, and penetration testing.

Assessment Methods

Penetration testing is testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. This type of testing can involve launching real attacks on real systems and data, using tools and techniques commonly used by attackers. Most penetration tests look for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability.

External penetration testing is conducted from outside the organization's security perimeter. This testing enables the tester to view the security features of an application, system, or network as they appear outside the security perimeter—usually as seen from the internet—with the goal of revealing vulnerabilities that could be exploited by external attackers. "Black

box" penetration testing is a method of testing in which the security controls, defenses, and design of the item being tested are tested from the outside with little or no prior knowledge of internal workings.

We performed this audit to determine whether FHFA's security controls were effective to protect its network and systems against external threats. We performed a series of vulnerability assessments and penetration tests on FHFA's publicly accessible systems, including its public-facing website. To accomplish these tests, we gathered information from public sources and assessed vulnerabilities from an access point external to FHFA's network. This testing used a "black box" method: an assumption that we had no prior knowledge of FHFA's network other than FHFA's confirmation that the IP addresses we discovered from publicly available internet sources belonged to FHFA. We also performed a wireless assessment from outside FHFA's physically controlled space and an email social engineering test.

FACTS AND ANALYSIS

Our Scanning Tools Identified Two Medium Severity Vulnerabilities in FHFA's Internet-Facing Systems, But We Were Unable to Exploit Those Vulnerabilities to Gain Access to FHFA's Network

We performed vulnerability scanning of 376 of FHFA's internet-facing IP addresses and 2 Amazon Web Services IP addresses hosting FHFA's public website, using commercially available network vulnerability assessment and penetration testing tools. Our vulnerability scanning did not find any critical[1] or high severity vulnerabilities on any of these addresses. Our scanning identified two unique medium severity vulnerabilities related to an encryption protocol[2] and the use of web cookies.[3] However, we were not able to exploit these medium severity vulnerabilities to gain access to FHFA's systems and data with our tools. We provided the results of our vulnerability scanning to FHFA management. Regarding the

[1] Computer security vulnerabilities are rated using the NIST Common Vulnerability Scoring System V3 ratings (NIST 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.

[2] Encryption protocols provide a protected channel for sending data between two computers. Encryption is used to secure communications in a variety of online transactions (e.g., financial transactions, healthcare transactions, email, or social networking).

[3] A web cookie is a small piece of data stored on the user's computer that stores the user's session information while accessing a particular website.

outdated encryption protocol, FHFA management informed us during fieldwork that the current version of the software running on the machines at the reported addresses could not be enabled with the higher encryption protocol and the machines did not support the higher versions of the software required to support that protocol.[4] Following our discussions with management regarding the web cookie, FHFA reported that they enabled a system setting to address the web cookie vulnerability and provided us with documentation of the changed setting.

Penetration Testing of FHFA's Wireless Network Did Not Identify Vulnerabilities

A wireless network works by using radio signals that can easily penetrate plywood floors, drywall, and windows. If these signals extend to public spaces (e.g., sidewalks, courtyards), they can be used by anyone in those spaces to access the network.

A form of active attack that can exploit these signals is an "evil twin" rogue wireless access point. The rogue wireless access point in this attack appears to belong to the target of the attack (in this case, FHFA's wireless network) but is actually controlled by the attacker. The attacker then induces legitimate users of the target's wireless network to connect to the rogue wireless access point. Once connected, users access their regular accounts and conduct business as normal, but the attacker can view and manipulate the client devices' communications, as well as potentially gain access to the client devices themselves as a "man in the middle."[5]

We conducted penetration testing of FHFA's wireless networks and devices to determine whether or not they are vulnerable to external attackers. From outside of FHFA's Headquarters building, we attempted to access FHFA's internal wireless network. Due to weak signals, we were not able to connect to the internal wireless networks. As another test, we attempted to set up a rogue wireless access point to be used for man-in-the-middle attacks against FHFA-owned devices, such as notebooks and cell phones. Using a wireless penetration test device, we searched for FHFA-owned devices attempting to connect to FHFA's internal wireless network. If a connection attempt had been detected, the network information could have been used to perform additional penetration tests. Our device detected no FHFA-owned devices attempting to connect to FHFA's network during our test.

[4] After we completed our fieldwork, FHFA provided documentation that appears to show that the encryption protocol issue had been remediated after our scan.

[5] In a "man-in-the-middle" attack, the attacker positions himself or herself between two communicating parties to intercept and/or alter data traveling between them.

34% of Sampled FHFA Employees Failed Email Phishing Test

Prior to gaining access to FHFA information systems, all users must agree to FHFA's Rules of Behavior and annually reaffirm their agreement with these Rules. Among other things, the Rules caution users to [redacted] in emails received from unknown senders and to report suspicious emails to OTIM's Help Desk or through the "Report Phishing" feature in FHFA's email application. In addition, FHFA conducts phishing exercises to test the effectiveness of security awareness training and adherence to the Rules. FHFA reported to us that in September 2018, nearly [redacted]% of users appropriately reported a suspicious email from the latest phishing simulation it had conducted. However, [redacted]% of users [redacted] in the suspicious emails.

As part of our audit and using our commercially available automated tool, we conducted an email phishing test on a sample of 50 FHFA employees with the [redacted] according to publicly available data.[6] We crafted and sent to these 50 employees an email that claimed to have details on [redacted]. [redacted] The page at the [redacted]. Our tool reported that 17 employees (34%) [redacted]. FHFA management provided us with documentation showing that 3 of the 50 FHFA users in the sample reported our phishing email to FHFA's security team.

FINDINGS .....

Some of FHFA's Internet-Facing Systems Were Installed with Outdated Encryption Protocols

We found that an outdated encryption protocol was in use on some of FHFA's internet-facing systems in contravention of NIST SP 800-52 Revision 1.[7] FHFA staff informed us that the systems in question were incapable of running any newer versions of the encryption protocol and need to be upgraded. FHFA staff also stated those systems were near the end of their service life and were due to be replaced in [redacted] 2019.

[6] Our sample excluded FHFA employees who had IT in their job title or were FHFA-OIG employees.

[7] [redacted]

FHFA Employees Were Susceptible to Email Phishing

Our email phishing test revealed that FHFA employees are still susceptible to email phishing attacks. Our test resulted in 34% of sampled employees [redacted] to access a website we had established for the test and only 6% reporting the email as suspicious. The FHFA Information System Rules of Behavior and User Acknowledgement states that FHFA users are responsible for [redacted] in emails and reporting suspicious emails.

CONCLUSION

We found that FHFA's security controls prevented our attempts from gaining unauthorized access to its systems and FHFA's website hosted by Amazon Web Services. That said, our vulnerability assessment from outside of FHFA's network discovered two medium severity vulnerabilities. FHFA addressed one of these vulnerabilities – servers using a web cookie without recommended security protection – during our audit. FHFA provided documentation that appears to show that the other vulnerability – an outdated encryption protocol – was remediated and advised that existing systems will be replaced in [redacted] 2019. Our phishing email test resulted in 34% of sampled FHFA employees [redacted] we established for this test. Accordingly, continued emphasis to employees to [redacted] in emails is warranted.

RECOMMENDATIONS

We recommend that FHFA:

1. Ensure planned systems replacements meet NIST SP 800-52 Revision 1 requirements for encryption.

2. Emphasize to employees the need to [redacted] in emails and report suspicious emails.

3. Continue to perform periodic phishing email tests.

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

the recommendations. FHFA stated that it had already taken action to remediate the encryption protocol finding and provided us with documentation in support of the action it took. FHFA also stated that it would ensure, during the acquisition process, that future system replacements meet the NIST SP 800-52 Revision 1 requirements for encryption. With regard to our finding that FHFA emphasize to employees the need to [redacted] in emails and report suspicious emails, FHFA agreed to evaluate its latest phishing email test results by June 30, 2019, to determine if its end user phishing email training needs to be enhanced and to implement a warning banner on incoming email messages that originate from non-FHFA email by March 31, 2019. FHFA also agreed to continue to perform quarterly phishing email tests during fiscal year 2019, and ad hoc phishing email tests to specific sub-groups during fiscal year 2019. We consider FHFA's reportedly completed and planned corrective actions responsive to our recommendations.

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 external threats. We performed an external security assessment of FHFA's IT systems that can be accessed from the internet, a wireless assessment from outside FHFA's physically controlled space at its Headquarters building, and an email phishing[8] test to assess whether FHFA employees are susceptible to social engineering[9] attacks.

For our external security assessment of FHFA's IT systems that can be accessed from the Internet, using publicly available sources we identified internet addresses assigned to FHFA, which FHFA management confirmed. We used automated commercial off-the-shelf software products in tandem with manual methods (i.e., using built-in operating system functions and commands) to gather information about FHFA's internet-facing systems and tested specific vulnerabilities in those systems. We also performed several tests of FHFA's wireless networks inside and around its Headquarters building.

We conducted our external security assessment of FHFA's IT systems in four phases: discovery, vulnerability assessment, exploitation, and reporting. During the discovery phase, we gathered information from the internet outside of FHFA's network and facilities to identify potential targets and obtain unprotected data about those targets. To find and map

[8] Phishing is the use of fraudulent emails or texts, or copycat websites to get a user to share personal information, such as account numbers, login IDs, or passwords.

[9] Social engineering is the act of tricking someone into divulging information or taking action, usually through technology.

FHFA's systems accessible from the internet, we used our licensed software (i.e., [redacted]) to conduct automated scanning and standard operating system functions (e.g., ping, traceroute) to manually verify specific situations. The vulnerability assessment phase focused on checking FHFA's internet-facing systems and public websites for known security vulnerabilities. During the exploitation phase, we attempted to gain unauthorized access to FHFA systems using the vulnerabilities discovered. The reporting phase was the final phase, where we analyzed and compiled our test results then provided them to Agency management. We also met with management to confirm reported vulnerabilities and false positives. We did not include false positives in our report.

An intrusion would have been considered successful if we had gained access to FHFA systems or data, which should have been denied, allowing us the ability to view/copy data, monitor user activities, install programs in memory, or otherwise control the target. As is a recommended practice by NIST, we entered into a Rules of Engagement with FHFA management that outlined the general parameters and period of our testing, and protocols for reporting any successful intrusions. In line with the Rules of Engagement, we only attempted to exploit vulnerabilities during FHFA's core business hours.

For our wireless penetration test, we used a directional antenna pointed at the FHFA Headquarters building and walked around the perimeter of the building to identify any FHFA wireless networks that were strong enough for a device outside the building to connect. We discovered a weak signal associated with FHFA's two untrusted wireless networks, those used to provide internet access to non-FHFA-owned computers and mobile devices, but no signal for our device to connect to FHFA's internal network. Additionally, we used the [redacted]®, a commercially available wireless testing device, to induce FHFA-owned devices to connect to the device by pretending to be the FHFA network. In the test, we placed the device in the FHFA Headquarters building lobby during the morning rush hour. The device logged any wireless access points it could detect and attempts by passers-by to connect to any wireless network. We obtained information from 143 unique mobile devices and wireless access points, including names for two FHFA networks intended for guests and personally owned devices. However, we did not have sufficient information on FHFA's internal wireless networks to reconfigure the device specifically to masquerade as an FHFA wireless network.

For our email phishing test, we used a commercial penetration test tool to send out a phishing email to a sample of FHFA employees. The email was designed to encourage employees into opening the email, [redacted], and submitting information to establish an account with a fictional news website that we created for the purpose of this test. We selected the sample of employees by filtering a publicly available database of federal employees' [redacted] and selecting the 50 FHFA employees [redacted]. We excluded FHFA employees who had IT in their job title or were FHFA-OIG employees. [redacted]

[redacted][10]

An image of the email used for this test follows.

We conducted this performance audit between April 2018 and February 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.

[10] According to NIST, a variant of phishing is spear phishing where the adversary is aware of, and specific about, the victim's profile. More than a generic phishing email, a spear phishing email makes use of more context information to make users believer that they are interacting with a legitimate source.

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: Federal Housing Finance Agency's (FHFA) Response to FHFA Office of Inspector General Draft Audit Report, *External Penetration Test of FHFA's Network and Systems During 2018*

DATE: January 11, 2019

This memorandum provides FHFA's management response to the findings contained in the draft audit report *External Penetration Test of FHFA's Network and Systems During 2018*.

Recommendation 1: OIG recommends that FHFA:

1. Ensure planned systems replacements meet NIST SP 800-52 Revision 1 requirements for encryption.

FHFA Response: FHFA agrees with the recommendation and has taken or will take the following actions:

1. FHFA remediated the finding related to [redacted] by July 15, 2018; and
2. FHFA will ensure, during the acquisition process, that future system replacements meet NIST SP 800-52 Revision 1 requirements for encryption.

Recommendation 2: OIG recommends that FHFA:

1. Emphasize to employees the need to [redacted] in emails and report suspicious emails.

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

1. FHFA will evaluate its latest phishing email test results by June 30, 2019 to determine if its end user phishing email training need to be enhanced; and
2. FHFA will implement a warning banner on incoming email messages that originate from non-FHFA senders by March 31, 2019.

Recommendation 3: OIG recommends that FHFA:

1. Continue to perform periodic phishing email tests.

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

1. FHFA will continue to perform quarterly phishing email tests during Fiscal Year 2019; and
2. FHFA will continue to perform ad hoc phishing email tests to specific sub-groups during Fiscal Year 2019.

If you have any questions, please feel free to contact [redacted] at (202) 649-[redacted] or e-mail, [redacted].

CC: T. Leach
J. Major
R. Mosios
C. Sherman
J. Vercellone
E. Hall
D. Crites

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