Federal Housing Finance Agency
Office of Inspector General

FHFA Effectively Blocked Phishing Emails, But Requires Improvement in Managing Vulnerabilities on Its Public Websites

Audit Report • AUD-2023-008 • September 27, 2023

AUD-2023-008

September 27, 2023

Executive Summary

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the Federal Housing Finance Agency (FHFA or Agency), to develop, document, and implement an agency-wide program to provide security for the information and information systems that support the operations and assets of the agency, and to periodically test that program. Within FHFA, the Office of Technology and Information Management (OTIM) works with mission and support offices to promote the effective and secure use of information and systems.

To support our ongoing oversight of FHFA's compliance with FISMA, we periodically audit FHFA's networks and information security. The objective of this audit was to determine whether FHFA's security controls are effective to protect its network and systems against external threats. The scope of our audit included FHFA's internet-accessible information systems, including its public websites, and email phishing tests directed at samples of employees from March 1 through June 30, 2023. We conducted fieldwork for this audit from February through July 2023, at our headquarters in Washington, D.C.

During our testing period, we found that FHFA's spam protection security control at system entry effectively detected and blocked unsolicited emails. Notably, FHFA's email security tool successfully prevented our social engineering phishing emails, which were designed to trick users into opening malicious emails, from reaching users' mailboxes. We also identified areas for improvement in FHFA's management of vulnerabilities on its public websites. We found that FHFA did not adequately scan and remediate vulnerabilities in those sites. OTIM officials acknowledged relying on the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) to conduct quarterly vulnerability scans of FHFA's public websites, and noted that they were unaware of certain vulnerabilities identified by our tool because the CISA scans did not detect them. Unaddressed vulnerabilities increase the risk of hackers compromising the confidentiality, integrity, and availability of FHFA's public websites.

Additionally, we found that FHFA's policies and procedures did not fully define the process for monitoring, scanning, and remediating vulnerabilities on its public websites. OTIM officials did not provide a reason for this absence in their policies and procedures. The lack of documented guidelines may lead to inconsistencies in vulnerability monitoring and scanning procedures and could result in delayed remediation of vulnerabilities by FHFA.

AUD-2023-008

September 27, 2023

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

This report was prepared by Jackie Dang, IT Audit Director; Marcie McIsaac, IT Audit Manager; and Zachary Lewkowicz, Auditor-in-Charge; 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

CISA	Cybersecurity & Infrastructure Security Agency
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
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
OTIM	Office of Technology and Information Management
SP	Special Publication

BACKGROUND

Federal Standards for Information Security

FISMA requires agencies, including FHFA, to develop, document, 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. Prescribed 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 Special Publications (SP) as recommendations and guidance documents.

FISMA also requires Inspectors General to perform annual independent evaluations of their respective agencies' information security programs and practices to determine their effectiveness. For FHFA, these evaluations are performed by an independent external auditor under contract with the Office of Inspector General. For fiscal year 2023, the auditor concluded that collectively the Agency's information security programs and practices were effective and complied with FISMA and related information security policies and procedures, standards, and guidelines. Although the Agency implemented effective security programs and practices, a subset of selected controls was not fully effective.[1]

NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* (September 30, 2008), 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. These recommendations serve several purposes—such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (updated December 10, 2020), provides a comprehensive catalog of security and privacy controls to meet current and future protection needs based on changing threats, vulnerabilities, requirements, and technologies. The relevant NIST SP 800-53 technical specifications require that federal agencies perform the following activities:

[1] FHFA-OIG, *Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2023* (July 26, 2023) (AUD-2023-004).

- Employ spam[2] protection mechanisms at system entry and exit points to detect and act on unsolicited emails.
- Monitor, scan, and remediate vulnerabilities in systems and applications within organizationally defined timeframes and processes.
- Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process.
- Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.[3]

FHFA's Standards and Guidelines for Vulnerability Management

FHFA has several written policies and procedures that govern its processes related to information security that include its vulnerability management process. Specifically, OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022), has established target remediation timeframes based on vulnerability severity rating. The process requires that externally accessible medium non-exploitable[4] vulnerabilities are remediated within 120 days.

FHFA's Network and Systems

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;

[2] NIST defines spam as electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

[3] As per NIST, organizations have many options for responding to risk, including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk.

[4] 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.

- Ensure the security of FHFA information and systems; and
- Develop strategic plans and goals for using advances in data and technology.

FHFA's network and systems host a variety of data and information such as financial reports, data from Fannie Mae and Freddie Mac (the Enterprises), examinations and analyses of the regulated entities, and personally identifiable information of employees. Networks and systems connected to the internet provide access points and therefore pose unique risks to FHFA in safeguarding its information. FHFA implemented a security program that includes security testing and assessments for determining the effectiveness of security controls in safeguarding its information systems and unclassified information.[5]

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 by using common tools and techniques of 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.

We performed external penetration testing of FHFA's 58 internet-accessible information systems, including 20 public websites,[6] to determine whether FHFA's security controls were effective to protect its network and systems against external threats. To perform our testing, we gathered information from public sources and assessed vulnerabilities from an access point external to FHFA's network. We also performed three social engineering email phishing tests on samples of FHFA's employees.

[5] NIST defines controlled unclassified information as information that law, regulation, or government-wide policy requires 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.

[6] NIST defines a website as a set of related web pages that are prepared and maintained as a collection in support of a single purpose. Websites have a user interface and are meant to be used by humans.

FACTS AND ANALYSIS

FHFA Effectively Blocked Our Phishing Emails, But Requires Improvement in Managing Vulnerabilities on Its Public Websites

During our test period, we found that FHFA's spam protection security control at system entry effectively detected and blocked unsolicited emails. Specifically, we found that FHFA's email security tool successfully prevented the delivery of our social engineering[7] phishing emails[8] to users' mailboxes. In other areas, we identified vulnerabilities on FHFA's public websites and found that FHFA's policies and procedures lacked guidelines for monitoring, scanning, and remediating those vulnerabilities.

FHFA Did Not Adequately Scan and Remediate Vulnerabilities on Its Public Websites

We conducted web vulnerability scanning on FHFA's 58 internet-accessible information systems,[9] including FHFA's public websites, using commercially available vulnerability assessment and penetration testing tools. None of these systems had critical or high severity vulnerabilities[10] based on our scans. We identified five non-exploitable medium severity vulnerabilities in FHFA's public websites.

Upon receiving our scan reports, OTIM officials:

- Remediated two vulnerabilities;
- Determined one vulnerability to pose minimal risk to their operations that did not require further action;

[7] The NIST definition of social engineering states that it involves tricking someone into divulging information or taking action, usually through technology.

[8] Phishing, as defined by NIST, is a digital form of social engineering that utilizes authentic looking but bogus emails to request information from users or to direct them to a fake website that requests information.

[9] CISA defines internet-accessible information systems as any system that is globally accessible over the public internet and encompasses those systems directly managed by an organization, as well as those operated by a third-party on an organization's behalf.

[10] NIST utilizes its Common Vulnerability Scoring System v3 (CVSS) to rate computer security vulnerabilities. The CVSS ratings are based on a 10-point scale, taking into account the likelihood and consequences of someone exploiting the vulnerability. Vulnerabilities with CVSS base scores of 9.0 or higher are considered critical severity; scores ranging from 7.0 to 8.9 are high severity; scores from 4.0 to 6.9 are medium severity; and scores from 0.1 to 3.9 are low severity. A score of 0 represents a severity level of none.

- Deemed one vulnerability as a false positive,[11] and chose not to pursue any further action; and

- Plan to accept the risk for the one remaining vulnerability, which was initially discovered on the May 12, 2021, CISA report.

While we confirmed OTIM's actions for four of the five vulnerabilities noted above, we found that OTIM did not document its risk acceptance for the last vulnerability as required by NIST SP 800-53. OTIM officials did not explain why they did not document the risk acceptance for this vulnerability. They stated that they will not take any further action to remediate the vulnerability but will accept the risk because they believe that it is low. Subsequent to the end of fieldwork, OTIM provided documentation of risk acceptance for this vulnerability. As such, we made no recommendation related to this finding.

We also discovered that FHFA owns two vulnerability scanning tools but did not utilize them to scan for vulnerabilities on its public websites, as required by NIST SP 800-53. One tool is the same as used by CISA for its quarterly vulnerability scans of FHFA's public websites. Because it owned a different tool,[12] OTIM had the capability to use it to scan its public websites for vulnerabilities that might not have been identified by the CISA tool.

OTIM officials explained that they rely on CISA to conduct quarterly vulnerability scans on FHFA's public websites.[13] They justified this approach by stating that running its own scans would be redundant, as FHFA would use the same scanning tool as CISA. However, as noted above, OTIM does have a scanning tool different from the one employed by CISA. OTIM officials stated that they were not aware of some of the vulnerabilities that our tool identified because the CISA scan reports they relied on did not identify these vulnerabilities.

Unaddressed vulnerabilities pose an increased risk of hackers compromising the confidentiality, integrity, and availability of FHFA's public websites. Our vulnerability scan results demonstrated that there were vulnerabilities not identified by CISA's quarterly scans. By using its own scanning tools, OTIM might have identified additional vulnerabilities that were not reported by CISA, and OTIM officials could have been aware of the risks to its public websites. Without this awareness, FHFA's public websites could be at risk of compromise for an extended period of time.

---

[11] Based on our review, we concluded that this vulnerability is a false positive, and NIST defines a false positive as an alert that incorrectly indicates that a vulnerability is present.

[12] OTIM uses this tool to scan other systems but not the public websites.

[13] FHFA provided web vulnerability scan reports of FHFA's public websites conducted by CISA in February 2023 and May 2023.

FHFA's Policies and Procedures Did Not Fully Define the Process for Monitoring, Scanning, and Remediating Vulnerabilities on Its Public Websites

We found that FHFA's policies and procedures did not fully define the process for managing vulnerabilities on its public websites, as required by NIST SP 800-53. OTIM Vulnerability Management Process, Revision 2.7 (September 7, 2022), aims to provide a formal, focused, and coordinated approach to proactively identify, manage, and mitigate information system vulnerabilities. This document did not define the process for monitoring, scanning, and remediating vulnerabilities on its public websites.

OTIM officials stated that OTIM General Support System (GSS) Information Security Architecture, Revision 2.5 (May 21, 2021), refers to the CISA scans. This document states that DHS conducts quarterly vulnerability scans of FHFA's public websites. However, this document did not define the process for monitoring, scanning, and remediating the vulnerabilities. Furthermore, OTIM officials could not explain why OTIM Vulnerability Management Process document did not define the process for monitoring, scanning, and remediating vulnerabilities on its public websites.

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*[14] states that management should implement control activities through policies. Management for the unit may further define policies through day-to-day procedures. Procedures may include the timing of when a control activity occurs and any follow-up corrective actions to be performed by competent personnel if deficiencies are identified. Management communicates to personnel the policies and procedures so that personnel can implement the control activities for their assigned responsibilities.

The absence of documented policies and procedures that accurately reflect the current vulnerability management process increases the risk of inconsistencies in FHFA's vulnerability monitoring and scanning procedures. Additionally, it may result in delays in remediating vulnerabilities in a timely manner.

FINDINGS

- FHFA did not adequately scan and remediate vulnerabilities on its public websites, and in one instance, did not document its risk acceptance for one vulnerability, as required by NIST SP 800-53.

[14] GAO-14-704G, *Standards for Internal Control in the Federal Government* (September 10, 2014).

- FHFA's policies and procedures did not fully define the process for managing vulnerabilities on its public websites, as required by NIST SP 800-53.

CONCLUSIONS

FHFA effectively implemented spam protection security control, safeguarding its network and systems against external threats. We found vulnerabilities in FHFA's websites of which OTIM was unaware, because it was not using its own scanning tool. Without OTIM's awareness, there may be increased risk of hackers compromising the confidentiality, integrity, and availability of FHFA's information and systems. Further, the lack of a defined process in FHFA's policies and procedures for monitoring, scanning, and remediating vulnerabilities on its public websites could result in inconsistencies and hinder timely resolution of these issues.

RECOMMENDATIONS

We recommend that the FHFA Acting Chief Information Officer:

1. Utilize OTIM's existing vulnerability scanning tool to supplement CISA scan reports to identify vulnerabilities not captured by CISA's scanning tool.

2. Define the process for monitoring, scanning, and remediating vulnerabilities on its public websites in OTIM Vulnerability Management Process document, including utilizing OTIM's existing vulnerability scanning tool to scan its public websites.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA management an opportunity to respond to a draft of this audit report. FHFA management provided a technical comment on the draft report and that comment was considered in finalizing this report. FHFA management also provided a written management response, which we included as an Appendix to this report. In its management response, FHFA agreed with our recommendations and included the following planned corrective actions:

1. FHFA will utilize its existing vulnerability scanning tool to scan its public websites and provide evidence of the completed scans by December 31, 2023.

2. FHFA will update its Vulnerability Management Process to define the process for monitoring, scanning, and remediating public website vulnerabilities by February 29, 2024.

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

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective for this audit was to determine whether FHFA's security controls were effective to protect its network and systems against external threats. The scope of our audit was comprised of FHFA's internet-accessible information systems, including its public websites, and samples of employees to conduct email phishing for the period March 1 through June 30, 2023.

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 internal control activities component was significant to this objective. It focused on the underlying principle that management should design the security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system.

- 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,[15] which is a recommended practice by NIST. In line with the Rules of Engagement, we only attempted to exploit vulnerabilities during FHFA's core business hours.

- Conducted our external security assessment of FHFA's public websites in four phases: discovery, vulnerability assessment, exploitation, and reporting.

  - Discovery phase: 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 FHFA's public websites, we used our licensed software to conduct automated scanning and standard operating system

[15] 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/copy data, monitor user activities, install programs in memory, or otherwise control the target.

functions (e.g., ping, traceroute) to manually verify specific situations. We discovered 58 FHFA internet-accessible information systems that included 20 public websites. We used a "black box" method, which is an assumption that we had no prior knowledge of FHFA's network other than FHFA's confirmation that the targeted systems we discovered from the internet belonged to FHFA.

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

  - Exploitation phase: Attempted to gain unauthorized access to FHFA systems using the vulnerabilities discovered.

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

- After confirming the vulnerabilities with FHFA management, reviewed the following FHFA policies and procedures to determine FHFA's security controls and process for vulnerability management:

  - FHFA Common Control Plan, Revision 3.4 (July 16, 2021)

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

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

- Interviewed the OTIM Principal IT Specialist and Senior IT Specialist on remediation of vulnerabilities identified and FHFA's security controls.

- Conducted email phishing tests using an open-source penetration test tool in three separate phishing email scenarios. We performed the following:

  - Designed three emails to encourage employees to open the email, click on hyperlinks, and submit information into fictional websites.

  - Gathered a list of FHFA employee names and job titles from a publicly available database of federal employees. We removed FHFA employees who had IT in their job title or were FHFA-OIG employees from this list and verified their email addresses. From the total population of 562 employees, we selected three samples for three phishing email scenarios, each with a sample size of 85 employees (approximately 15 percent of the population) using a random number generator. We used this methodology for the purpose of avoiding bias and not

for the purpose of projecting results across the population. Each sample included three employees in FHFA leadership.

- Obtained and reviewed FHFA Information System Rules of Behavior and User Acknowledgement (December 6, 2022) and the annual IT security and privacy awareness training materials to determine whether the Rules of Behavior and training materials contain guidance for preventing social engineering attacks.

- Obtained and reviewed FHFA email logs and interviewed an FHFA Principal IT Specialist to determine how FHFA's email security tool successfully prevented our social engineering phishing emails from reaching users' mailboxes.

We conducted this performance audit between February 2023 and September 2023, 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: 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: Katrina D. Jones, Chief Operating Officer

KATRINA JONES
Digitally signed by KATRINA JONES
Date: 2023.09.06 16:05:13 -04'00'

FROM: Tammie L. Tippie, Acting Chief Information Officer

TAMMY TIPPIE
Digitally signed by TAMMY TIPPIE
Date: 2023.09.06 15:43:31 -04'00'

SUBJECT: Draft Audit Report: *FHFA Effectively Blocked Phishing Emails, But Requires Improvement in Managing Vulnerabilities on Its Public Websites*

DATE: September 6, 2023

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

Recommendation 1: *Utilize OTIM's existing vulnerability scanning tool to supplement CISA scan reports to identify vulnerabilities not captured by CISA's scanning tool.*

Management Response to Recommendation 1: FHFA agrees with the recommendation and will utilize its existing vulnerability scanning tool to scan its public websites and provide evidence of the completed scans by December 31, 2023.

Recommendation 2*: Define the process for monitoring, scanning, and remediating vulnerabilities on its public websites in OTIM Vulnerability Management Process document, including utilizing OTIM's existing vulnerability scanning tool to scan its public websites.*

Management Response to Recommendation 2: FHFA agrees with the recommendation and will update its Vulnerability Management Process to define the process for monitoring, scanning, and remediating public website vulnerabilities by February 29, 2024.

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

cc: Edom Aweke
Tom Leach
Ralph Mosios
John Major

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