Federal Housing Finance Agency
Office of Inspector General

Inspection: FHFA's Adherence to Cyber Incident Reporting Procedures

Inspection • COM-2024-009 • July 30, 2024

EXECUTIVE SUMMARY

PURPOSE

In December 2021, FHFA adopted Cyber Incident Reporting Procedures (Cyber Procedures) for reporting certain information about security incidents to the Department of Homeland Security's Computer Emergency Readiness Team (US-CERT). This inspection's objective was to assess whether – and if so, to what extent – FHFA adhered to the Cyber Procedures' tracking requirements from January 1, 2022, through December 31, 2023 (review period).

RESULTS

The materials reviewed show that FHFA generally followed its Cyber Procedures from January 1, 2022, through December 31, 2023. FHFA documented incidents it reported to US-CERT during the review period and maintains documentation for the incidents listed on its tracking spreadsheet.

However, the tracking spreadsheet contains date inaccuracies. Specifically, for 33 percent of the reported incidents (three of nine), the tracking spreadsheet lists report dates that differ from the dates reflected in each US-CERT receipt confirmation email. Such inaccuracies could impact FHFA's future Federal Information Security Modernization Act of 2014 (FISMA) submissions to Congress.

RECOMMENDATION

Update OTIM's existing written procedures to include new controls or improve existing controls to ensure the accuracy of security incident records, and train staff on the updated procedures.

FHFA agreed with the recommendation, and proposed to implement corrective actions by October 31, 2024, to remediate the deficiency referenced above.

This report was prepared by Kristopher Brash Dixon, Program Analyst, and Patrice Wilson, Senior Investigative Evaluator. 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.

Brian W. Baker
Deputy Inspector General
Office of Compliance

TABLE OF CONTENTS

ABBREVIATIONS

Agency or FHFA	Federal Housing Finance Agency
Cyber Procedures	Cyber Incident Reporting Procedures
FISMA	Federal Information Security Modernization Act of 2014
IT	Information Technology
OIG	FHFA Office of Inspector General
OTIM	FHFA Office of Technology & Information Management
Review Period	January 1, 2022 – December 31, 2023
US-CERT	U.S. Computer Emergency Readiness Team

BACKGROUND

Federal Standards for Incident Reporting

In September 2003, the U.S. Department of Homeland Security's cyber security division created US-CERT to protect the nation's internet infrastructure by coordinating defense against, and response to, cyber-attacks.[1] US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating responses to information security incidents (hereafter, security incidents or incidents).

FISMA defines an incident as an occurrence that either:[2]

- Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

FISMA requires federal civilian executive branch agencies to submit reports directly to Congress detailing major security incidents, both as they occur and annually.[3] In addition, agencies must notify and consult with US-CERT regarding information security incidents involving those agencies' information and information systems.[4]

Pursuant to its authority under FISMA, US-CERT established notification guidelines requiring civilian executive branch agencies to report security incidents where the confidentiality, integrity, or availability of the agency's information system is potentially compromised. US-CERT expects agencies to file these reports within one hour after identifying the incident.[5] After US-CERT receives a report, it provides the agency with email confirmation of receipt. In addition, agencies are required to submit an annual report to Congress that includes the total number of security incidents over the preceding year.

---

[1] In 2023, US-CERT was retired and its functions were incorporated into the Cybersecurity and Infrastructure Security Agency (CISA). However, for ease of reference, and since the Agency's Cyber Procedures continue to refer to US-CERT, this report refers to the relevant entity as US-CERT.

[2] 44 U.S.C. § 3552(b)(2).

[3] *Id.* §§ 3554(b)(7)(C)(iii)(III), 3554(c)(1).

[4] *Id.* § 3554(b)(7)(C)(ii).

[5] The notification guidelines permit an agency to also report incidents voluntarily to US-CERT that it found did not impact confidentiality, integrity, or availability. CISA, *US-CERT Federal Incident Notification Guidelines* (eff. April 1, 2017).

FHFA's Information Technology Security Program

FHFA's Office of Technology and Information Management (OTIM) works with the Agency's mission and support offices to manage the Agency's technology resources and to ensure the security of FHFA information and systems.[6] OTIM is also responsible for determining whether a security incident must be reported to US-CERT and, in such cases, for making the report.

OIG's Audit and OTIM's US-CERT Reporting Procedures

In a 2021 audit report, OIG found that OTIM did not record or track all security incidents that FHFA said it had reported to US-CERT.[7] We recommended that the Agency establish "written procedures that define: (a) the pertinent information that needs to be recorded, tracked, and reported for all security incidents and (b) the controls to ensure the accuracy and completeness of the security incident records." The Agency rejected our recommendation because it asserted that their *Information Security Incident and Personally Identifiable Information Breach Response Plan* addressed the recommendation; FHFA stated that it would take no further action.[8]

Nevertheless, in December 2021, OTIM adopted its Cyber Procedures,[9] which implement the US-CERT reporting requirement by establishing FHFA's process for handling reportable incidents – more specifically, the process by which OTIM must assess information to determine whether an incident is required to be reported to US-CERT.[10] The Cyber Procedures require OTIM to report an incident to US-CERT after assessing several factors, including but not limited to whether the incident impacted FHFA systems' confidentiality, integrity, or availability.

Once OTIM reports an incident to US-CERT, the Cyber Procedures require OTIM to track that incident in a spreadsheet. OTIM's spreadsheet is designed to include the following information for each reported incident: (1) the incident date; (2) the report number assigned by US-CERT to

---

[6] FHFA's information technology (IT) 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 Agency employees' personally identifiable information.

[7] OIG, *FHFA Did Not Record, Track, or Report All Security Incidents to US-CERT; 38% of Sampled FHFA Users Did Not Report a Suspicious Phone Call Made to Test User Awareness of its Rules of Behavior* (June 25, 2021) *(*AUD-2021-009*)*.

[8] FHFA's *Information Security Incident and Personally Identifiable Information Breach Response Plan* implements the requirement that incident response controls must be put into place to monitor and detect security events on a computer or computer network and to ensure the execution of proper responses to those events.

[9] Although elements of the Cyber Procedures are similar to what OIG recommended in the 2021 audit report (e.g., tracking), the Agency did not purport to be implementing our recommendation; indeed, as reflected in our findings, issues identified in that report have yet to be resolved.

[10] In March 2023, OTIM updated the Cyber Procedures and made minimal changes.

that incident; (3) OTIM's source(s) of information regarding the incident; (4) whether any follow-up is required; (5) a summary of the incident; and (6) comments.[11]

There are three ways that OTIM becomes aware of a potential reportable incident:

1. Automated Alerts from FHFA's IT System

OTIM officials report that each week they receive thousands of automated alerts regarding potential incidents (e.g., malware,[12] malicious links in emails, internal attacks against Active Directory[13] infrastructure, malware during routine scans) from several security platforms.[14] FHFA categorizes the severity of automated alerts according to the following scale: informational, low, medium, high, and critical. According to OTIM officials, the vast majority of automated alerts do not rise to being categorized as an incident and include such things as unsuccessful attempts (i.e., blocked by the firewall) to access Agency systems.

OTIM manually reviews a daily report of automated alerts with a severity level of high and critical. It also monitors alerts at other severity levels to ensure that none of the FHFA systems potentially targeted in an incident were impacted and that the incident was not a reconnaissance attack.[15]

2. Users, Helpdesk, and Management Input

Another way OTIM may become aware of reportable incidents is through users, the Helpdesk, or management submitting emails, support tickets, or phone calls of suspected malware.

3. Third-Party Reports

A third way OTIM may become aware of reportable incidents is through security reports and alerts from partner organizations (including OIG and US-CERT) and from vendors. According

---

[11] The Cyber Procedures also require OTIM to retain any records associated with an incident in accordance with FHFA's Comprehensive Records Schedule for a period of seven years after closure of the incident.

[12] Malware is any software used to gain unauthorized access to IT systems to steal data, disrupt system services, or damage IT networks.

[13] Active Directory is a database (i.e., an organized collection of data) and set of services that connects users with network resources they need to get their work done. An Active Directory can contain critical information about a system, including the identity of those users or computers accessing the system.

[14] Security platforms are automated tools for managing and securing FHFA's data, users, and network. Security platforms also notify OTIM of potential threats to FHFA's network. For example, FHFA's Security Information and Event Management System is one of the security platforms and it identifies unusual or suspicious events across FHFA's network for OTIM to potentially investigate.

[15] A reconnaissance attack occurs when an attacker gathers IT information about a target system before launching an attack.

to OTIM, most third-party reports are from US-CERT to alert FHFA of a potential threat. For example, a third-party report can include a report of "FHFA information" appearing on the dark web,[16] or exploits targeted at FHFA.[17]

Regardless of the source, the Cyber Procedures may require a submission to US-CERT depending upon OTIM's analysis of the information. For example, if OTIM analyzes a report of exploits targeted at FHFA, determines the exploit was successful, and concludes the confidentiality, integrity, or availability of FHFA systems were impacted, the Cyber Procedures require a submission to US-CERT.

The Cyber Procedures do not require OTIM to report lost Agency digital equipment (laptops, iPhones, and iPads) to US-CERT due to protection measures that OTIM says it has implemented on that equipment.[18] Despite this, US-CERT encouraged OTIM to report the lost equipment as a precaution, and OTIM does so.

OBJECTIVE AND SCOPE

Our inspection's objective was to assess whether and to what extent FHFA adhered to the Cyber Procedures' tracking requirements for incidents reported to US-CERT. The assessment focused on the period from January 1, 2022, through December 31, 2023 (the review period).

RESULTS

We determined that FHFA generally followed its Cyber Procedures during the review period. Specifically, based on the materials we reviewed, OTIM documented on its tracking spreadsheet all incidents it reported to US-CERT during the review period, and it maintains documentation for these incidents. However, the spreadsheet does not accurately track some of the incidents reported to US-CERT. Inaccuracies in Agency records could impact FHFA's future FISMA submissions to Congress.

[16] The term "dark web" refers to parts of the internet that require specific software to access. People can use the dark web for legitimate reasons such as private communication; however, many people use the dark web for criminal activities.

[17] An exploit is a computer program designed to find and take advantage of a security flaw or vulnerability in a computer system.

[18] OTIM reports that the information stored on FHFA laptops is protected by whole disk encryption. In addition, OTIM states that they can remotely wipe (i.e., OTIM is able to erase the data on those devices) lost or stolen iPhones and iPads. Consequently, the loss of such items does not pose a threat to the confidentiality, integrity, or availability of FHFA systems.

We are reporting two findings.

Finding 1: FHFA Tracks and Maintains Documentation for All Incidents It Reported to US-CERT During the Review Period

FHFA's tracking spreadsheet indicates that OTIM reported nine incidents to US-CERT during the review period.[19] Six of these reported incidents pertained to lost or stolen equipment.[20] Two of the reported incidents were based on reports OTIM received from US-CERT itself (i.e., were third-party reports), including one report of Agency information found on the dark web. Another of these reported incidents pertained to Controlled Unclassified Information that the Agency published inadvertently on its public website.[21] FHFA's Division of Enterprise Regulation reported this incident to OTIM.

We requested documentation for each of the nine submissions to US-CERT. OTIM provided documentation for all of them.

Finding 2: FHFA Recorded Several Incident Dates Inaccurately in the Tracking Spreadsheet

OTIM's tracking spreadsheet contains several date inaccuracies. Six of the nine incidents have incident dates on the tracking spreadsheet that match the date OTIM received the US-CERT confirmation email. However, for three (i.e., 33 percent) of the nine incidents, the incident date differs from the date reflected in US-CERT's confirmation email, as noted below:

- Incident 1 – The incident date on the tracking spreadsheet lists September 2022. However, OTIM received the US-CERT confirmation email in June 2022, which is earlier than the incident date listed on the tracking spreadsheet.

- Incident 2 – The incident date on the tracking spreadsheet lists August 2023. However, OTIM received the US-CERT confirmation email in November 2022, which is significantly earlier than the incident date listed on the tracking spreadsheet.

- Incident 3 – The incident date on the tracking spreadsheet lists November 2022. However, OTIM received the US-CERT confirmation email in August 2023, which is much later than the incident date listed on the tracking spreadsheet.

[19] According to OTIM, they did not report any automated alerts to US-CERT.

[20] As noted above, OTIM officials told us that even though their Cyber Procedures do not require them to report lost equipment, they do so as a precaution.

[21] Controlled Unclassified Information is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies.

While the date an incident is reported to US-CERT is dependent on when the Agency discovers the incident and may differ from the date the incident occurred, this does not explain the inaccuracies where OTIM received the US-CERT confirmation email months before the purported incident date listed on the tracking spreadsheet. When asked about these data inaccuracies, OTIM stated that they were data entry mistakes and provided an updated tracking spreadsheet.

The tracking spreadsheet's inaccuracies would not have impacted the Agency's annual FISMA report to Congress covering the review period, because the incident dates (the erroneous dates on the tracking spreadsheet and the dates of the receipt confirmation emails) while inaccurate, nonetheless were reported in the correct fiscal year. However, potential tracking spreadsheet mistakes in the future could cross fiscal years, resulting in the Agency reporting inaccurate incident totals to Congress.

Recommendation

1. We recommend that OTIM update its existing written procedures to include new controls or improve existing controls to ensure the accuracy of security incident records, and train staff on the updated procedures.

FHFA COMMENTS AND OIG EVALUATION.....

We provided a draft of this report to FHFA for its review and comment. The Agency's comments are included in the Appendix to this report. FHFA states that OTIM will update the existing written procedures by October 31, 2024, to include new controls or improve existing controls to ensure the accuracy of security incident records, and will train staff on the updated procedures.

We consider FHFA's planned corrective actions responsive to our recommendation. We will close the recommendation upon reviewing the documentation that FHFA committed to provide by October 31, 2024, and independently determining that FHFA has implemented corrective actions addressing all aspects of the open recommendation.

APPENDIX I: METHODOLOGY

To accomplish our objective, we performed the following procedures:

- We reviewed documentation of each incident reported to US-CERT in the tracking spreadsheet along with evidence of each submission.
- We interviewed OTIM officials.
- We conducted our inspection from April 2024 through May 2024 under the authority of the Inspector General Act of 1978, as amended, and in accordance with the *Quality Standards for Inspection and Evaluation* (December 2020), which were promulgated by the Council of the Inspectors General on Integrity and Efficiency.
- We provided a draft of this report to FHFA for its review and comment.

APPENDIX II: FHFA MANAGEMENT RESPONSE.....

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

Federal Housing Finance Agency

DRAFT-MEMORANDUM

TO: Brian Baker, Deputy Inspector General Office of Compliance

THRU: Katrina D. Jones, Chief Operating Officer

MARY PETERMAN Digitally signed by MARY PETERMAN Date: 2024.07.16 16:41:28 -04'00'

FROM: Luis Campudoni, Chief Information Officer

THOMAS LEACH Digitally signed by THOMAS LEACH Date: 2024.07.16 10:56:04 -04'00'

SUBJECT: Draft Inspection Report: FHFA's Adherence to Cyber Incident Reporting Procedures

DATE: July 16, 2024

Thank you for the opportunity to respond to the above-referenced draft audit report (Report) by the Office of Inspector General (OIG), which contains one recommendation. This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the recommendation, which is being managed by the Office of Technology and Information Management (OTIM).

Recommendation 1: *We recommend that OTIM update its existing written procedures to include new controls or improve existing controls to ensure the accuracy of security incident records, and train staff on the updated procedures.*

FHFA's Recommendation 1 Response: FHFA agrees with Recommendation 1. OTIM's Management Information Security Section will update its existing written procedures to include new controls or improve existing controls to ensure the accuracy of security incident records, and train staff on the updated procedures, by October 31, 2024.

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

cc: Edom Aweke
Tom Leach
Ralph Mosios
John Major
Warren Hammonds

Federal Housing Finance Agency
Office of Inspector General

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write: FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219