REDACTED

Federal Housing Finance Agency
Office of Inspector General

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

This report contains redactions of information that is privileged or otherwise protected from disclosure under applicable law.

Audit Report • AUD-2021-009 • June 25, 2021

AUD-2021-009

June 25, 2021

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 and Freddie Mac (together, the Enterprises), and the Federal Home Loan Bank System (collectively, the regulated entities). Since 2008, FHFA has served as conservator of the Enterprises.

The Federal Information Security Modernization Act of 2014 (FISMA) requires FHFA to implement agency-wide information security programs, including procedures for detecting, reporting, and responding to security incidents. FISMA defines "incident" as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." Pursuant to FISMA, the Department of Homeland Security (DHS) has directed Executive Branch civilian agencies to notify the United States Computer Emergency Readiness Team (US-CERT) in the event of an incident. Reportable incidents can come in several forms, including denial of service attacks, email attacks, impersonation, or loss or theft of equipment. FHFA developed a standard for detecting and responding to security incidents as well as standards governing training, testing, and documentation. FHFA requires all users to "[i]mmediately report any suspected or potential security incidents" to support personnel.

We conducted this audit to assess FHFA's incident detection and response controls against standards and guidelines established by FHFA and the federal government. Our review period was fiscal years 2019 and 2020.

We found that FHFA followed its standards in the development, implementation, and communication of its Information Security Incident and Personally Identifiable Information Breach Response Plan (Incident Response Plan). We also determined that FHFA used an automated tool to correlate and analyze audit records across different repositories to gain organization-wide situational awareness, in compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (updated January 22, 2015). However, we determined that FHFA had not recorded, tracked, or reported all security incidents to US-CERT, as required by FISMA. Specifically, we found that FHFA did not maintain complete records of incidents and lacked written procedures for recording, tracking, or reporting security incidents. We also found that FHFA failed to

AUD-2021-009

June 25, 2021

contemporaneously document the results of a table-top exercise to test its incident response capability, as required by its standard. Finally, we conducted a test to assess whether sampled FHFA employees and contractors followed a requirement in the FHFA Information System Rules of Behavior (Rules of Behavior) to immediately report any suspected or potential security incidents or data breaches to FHFA's Office of Technology and Information Management (OTIM). This test – a phone call to FHFA users on their FHFA-assigned phones in which we informed the user of certain data breaches – found that 38% of sampled FHFA employees and contractors did not report this suspicious phone call, in disregard of this requirement.

Based on our findings in this audit, we make three recommendations in this report. In a written management response, FHFA disagreed with the first recommendation and agreed with the second and third recommendations.

This report was prepared by Jackie Dang, IT Audit Director, and Dan Jensen, Auditor-in-Charge; with assistance from Abdil Salah, Assistant Inspector General for Audits, and 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, Senior Audit Executive /s/

TABLE OF CONTENTS

ABBREVIATIONS

After Action Report	Annual Disaster Recovery Exercise After Action Report
CPIRP	Cybersecurity Privacy & Incident Response Program
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
Incident Response Plan	Information Security Incident and Personally Identifiable Information Breach Response Plan
IT	Information Technology
NIST	National Institute for Standards and Technology
OTIM	Office of Technology and Information Management
Regulated Entities	Enterprises, affiliates of the Enterprises, and the Federal Home Loan Bank System
Rules of Behavior	FHFA Information System Rules of Behavior
SIEM	Security Information and Event Management
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

BACKGROUND

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 of employees. FHFA's OTIM works with mission and support offices to promote the effective and secure use of information and systems.

Federal Standards for Incident Response and Reporting

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, including procedures for detecting, reporting, and responding to security incidents. In addition, FISMA requires agencies to implement periodic testing and evaluation of the effectiveness of security policies, procedures, and practices. Pursuant to FISMA, NIST prescribes standards and guidelines pertaining to federal information systems. In addition, NIST issues recommendations and guidance documents.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (updated January 22, 2015), sets forth the requirements for incident response, which includes incident handling, monitoring, and reporting. NIST also requires that the information system implements policies, procedures, and training for those who handle information security incidents. Last, NIST requires the affected organization to correlate and analyze audit records across different repositories to gain organization-wide situational awareness.

Pursuant to FISMA and predecessor law, the Department of Homeland Security (DHS) has directed Executive Branch civilian agencies to notify US-CERT[1] in the event of an incident. Reportable incidents can come in several forms, including denial of service attacks, email attacks, impersonation, or loss or theft of equipment.

[1] US-CERT, which is part of DHS, generates security alerts and advisories to maintain situational awareness across the federal government (on line ***here***).

FHFA Standards and Guidelines

Incident Response Standard

FHFA's Incident Response Standard, Revision 1.4 (issued in June 2014; last updated in May 2020), directs 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. That standard requires, among other things:

- FHFA employees and contractors report suspected security incidents immediately to the FHFA Help Desk.
- FHFA develops an incident response plan that includes preparation, detection and analysis, containment, eradication, and recovery, which is reviewed and approved by the FHFA Chief Information Security Officer and distributed to all personnel with incident response responsibilities.
- FHFA communicates the incident response plan changes to all personnel with incident response responsibilities.
- FHFA provides incident response training to members of the incident response team and Help Desk staff within one year of assuming an incident response role or responsibility, when required by information system changes, and annually thereafter.
- FHFA tests incident response capabilities annually using pre-defined tests to determine incident response effectiveness and document the results.
- FHFA tracks and documents agency security incidents.
- FHFA retains any audit records associated with a security incident for a period of seven years after the closure activities for the incident, as prescribed by FHFA's Comprehensive Records Schedule.

This standard seeks to put appropriate incident response security controls in place to meet federal requirements and information protection needs arising from other mission/business processes. The Incident Response Plan implements the requirements of the Incident Response Standard.

Security Operations Center Strategy

FHFA's Security Operations Center Strategy, version 1.4 (issued in June 2016; last updated in May 2020), establishes FHFA's strategy for monitoring agency security devices to detect and respond to potential incidents. To meet the NIST requirement to correlate and analyze audit

records across different repositories, FHFA's strategy calls for OTIM analysts to use a Security Information and Event Management (SIEM) tool[2] to collect network event records from across its network, such as firewall traffic, security events, and identified threats. FHFA's SIEM tool is an automated tool that identifies unusual or suspicious events by themselves, or in combination with other events, across FHFA's network. Unusual or suspicious events are grouped together in dashboards, allowing OTIM analysts to more easily identify events that may require follow-up.

FHFA Information System Rules of Behavior

FHFA users are required to sign the Rules of Behavior document, last updated in October 2018, when receiving a user account and annually thereafter. Among the rules, users are to "[i]mmediately report any suspected or potential security incidents, data breaches, or non-compliance with the [Rules of Behavior] to the Help Desk."

FACTS AND ANALYSIS

While FHFA Established and Maintained an Incident Response Plan and Used its SIEM Tool, It Did Not Record, Track, or Report All Security Incidents to US-CERT or Contemporaneously Document the Results of a Table-Top Exercise

As required by its Incident Response Standard, we found that FHFA: developed, maintained, and communicated FHFA's Incident Response Plan; and conducted annual table-top exercises and provided training through these exercises.

In prior audits, we found that the reports used for the [redacted] were incomplete, which diminished the effectiveness of the [redacted]. Specifically, we reported that FHFA did not [redacted] *See* OIG, *Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2020* (Oct. 20, 2020) (AUD-2021-001) (online ***here***); and OIG, *Audit of an FHFA Sensitive Employment-Related Case Tracking System: FHFA Followed its Access Control Standard, But its System Is Adversely Impacted by Two Security Control Weaknesses* (Mar. 29, 2021) (AUD-2021-006) (online ***here***). FHFA has committed that it will assess, by July 30, 2021, the [redacted] for analysis and correlation. With that caveat, we found that an OTIM analyst reviewed the SIEM tool reports and reported the results of his

[2] SIEM tools are a type of centralized logging software that facilitates aggregation and consolidation of audit log records from multiple information systems. These tools facilitate audit log records correlation and analysis, which assist an organization in determining the veracity and scope of potential attacks.

review to OTIM management, in accordance with FHFA's Security Operations Center Strategy.

FHFA Failed to Maintain Complete Records of Incidents

FHFA's Incident Response Standard requires that Agency security incidents be tracked and documented, and audit records associated with a security incident be retained for seven years after the closure activities for the incident.[3] In contravention of this standard and internal control, we found that OTIM lacked written procedures for recording, tracking, or reporting security incidents.

The responsible OTIM employee explained that whenever he became aware of a security incident, he recorded it on a spreadsheet (hereafter referred to as the incident tracking spreadsheet) and submitted a report to US-CERT. The incident tracking spreadsheet included columns for recording Incident Date, US-CERT number, and Incident Summary (e.g., lost iPhone). The incident tracking spreadsheet also included a column labeled Comments where FHFA usually listed the name of the person who lost the reported item.

Our review of the information on security incidents recorded by FHFA on its incident tracking spreadsheet was incomplete and FHFA was unable to provide us with documents relating to most of these incidents. For fiscal year 2019, 16 security incidents were recorded on OTIM's incident tracking spreadsheet, consisting of 15 lost iPhones and 1 lost laptop. We found:

- The incident tracking spreadsheet did not include a US-CERT number for any of the lost items recorded.

[3] Agency management is required by the *Standards for Internal Control in the Federal Government* (the Green Book), under the Control Activities component of internal control, to design control activities to achieve the Agency objectives (e.g., to monitor and detect security events, and response appropriately) and respond to risks (e.g., security events are not monitored or detected, or the response is not appropriate). Control activities include, for example, the prompt recording of transactions to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of the event from its initiation through its final classification in summary records. (The Green Book is published by the Government Accountability Office (GAO). *See* GAO-14-704G (Sept. 2014)).

- We were only able to determine, from other documentation provided to us by FHFA, that 4 of the 15 lost iPhones recorded on the incident tracking spreadsheet were reported to US-CERT.[4, 5]

- For these four lost iPhones, FHFA provided us with four confirmation emails from US-CERT, with a US-CERT number, that cross-referenced to an FHFA Help Desk ticket number for the lost item, and we were able to link the Help Desk ticket number to the reported lost iPhone on FHFA's incident tracking spreadsheet.

- We were unable to determine whether the remaining 11 lost iPhones were reported to US-CERT. No US-CERT number for those lost items was recorded on FHFA's incident tracking spreadsheet. While FHFA provided us with three other confirmation emails from US-CERT, none referred to an FHFA Help Desk ticket number or provided other information that would have enabled us to trace the confirmation emails to anything recorded on the incident tracking spreadsheet for those 11 iPhones.[6]

- For the laptop recorded as lost on FHFA's incident tracking spreadsheet, the incident tracking spreadsheet did not show that the incident was reported to US-CERT and FHFA could not produce documentation demonstrating that the loss of this laptop was reported to US-CERT.

We found that FHFA's incident tracking spreadsheet for fiscal year 2020 was also incomplete. That spreadsheet showed five security incidents: three were requests from

[4] As further evidence that the incident tracking spreadsheet for fiscal year 2019 was incomplete, FHFA provided us with a US-CERT email dated September 21, 2019, confirming the submission of an incident report related to loss of certain iPhones; that incident was not recorded on the incident tracking spreadsheet.

[5] In a technical comment to this report, FHFA asserted, citing US-CERT Incident Notification Guidelines (April 1, 2017), that iPhones lost by its employees were not required to be reported to US-CERT because they were encrypted. Pursuant to that guidance, agencies could, but were not required, to report events that did not impact confidentiality, integrity, or availability of data. Had FHFA followed this guidance, it would not have reported any of the encrypted lost iPhones. Instead, it reported 4 of the encrypted lost phones but not 11. It was unable to demonstrate whether it reported these lost 11 iPhones or explain the reasons that it reported some, but not all, of the lost iPhones.

We note that, pursuant to FISMA, agencies provide annual reports to OMB regarding the number of security incidents by "attack vector," including lost equipment. The April 2017 US-CERT Guidelines instructed agencies not to include voluntarily reported events in their annual FISMA reports. For fiscal year 2019, FHFA reported encrypted lost iPhones. Plainly, FHFA has not consistently followed these US-CERT Incident Notification Guidelines.

[6] The incident date for the earliest lost iPhone in fiscal year 2019 was reported on FHFA's incident tracking spreadsheet as March 23, 2019, but two of the US-CERT confirmation emails provided to us reported Incident Submit Dates of March 13 and March 21, 2019, both prior to FHFA's first recorded Incident Date.

US-CERT and two were lost laptops.[7] For the three US-CERT requests, the incident tracking spreadsheet and supporting documentation provided by FHFA showed details of the request and the actions taken. A US-CERT number was recorded by FHFA on the incident tracking spreadsheet for one missing laptop but not the other. For the missing laptop where a US-CERT number was not recorded, FHFA could not produce documentation to show that the incident was reported to US-CERT.[8]

FHFA Failed to Contemporaneously Document Meeting Minutes for its November 2018 Incident Response Table-Top Exercise

In accordance with its Incident Response Standard, we found that FHFA developed, maintained, and communicated its Incident Response Plan. FHFA also conducted the required annual incident response table-top exercise[9] and provided training to members of the incident response team and Help Desk staff. However, we found that the meeting minutes for the table-top exercise conducted in November 2018 were completed in December 2020, 25 months later and only after we brought up the issue during our audit fieldwork. An FHFA official characterized the failure to contemporaneously document the meeting minutes in accordance with FHFA's Incident Response Standard as an oversight.[10]

FHFA subsequently maintained that its Cybersecurity Privacy & Incident Response Program (CPIRP) does not fall under the jurisdiction of the Incident Response Standard and, accordingly, a 25-month delay in documenting the meeting did not run afoul of its Incident Response Standard. We note that FHFA has changed its position on this and other issues addressed in this audit. Like a number of its other contradictory statements, this change in position is not credible, for the following reasons:

---

[7] US-CERT reporting requirements were revised effective January 1, 2020, removing the need to report events where confidentiality, integrity, and availability of agency data were not actually or imminently jeopardized. With this change to the reporting requirements, an FHFA official stated that the Agency no longer reports lost iPhones because these devices are encrypted and the data can be remotely wiped; therefore, they view the risk that data could be recovered as extremely low.

[8] In a technical comment to a draft of this report, FHFA claimed that its Help Desk ticketing system, not the incident tracking spreadsheet, is its official system for recording lost equipment. This technical comment is inconsistent with information provided by FHFA during this audit and past audits and, for that reason, we do not credit it. FHFA has produced the incident tracking spreadsheet in response to our requests in this audit and for past FISMA audits as its record of security incidents reported by FHFA employees and contractors. We also note that FHFA's Help Desk ticketing system does not record the incidents reported to US-CERT.

[9] NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, states that table-top exercises are discussion-based events where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation.

[10] FHFA prepared meeting minutes for the table-top exercise conducted the following fiscal year.

- As part of this audit, we sought evidence that FHFA tested its incident response capabilities annually; FHFA provided us with its CPIRP table-top exercises. We found that meeting minutes for the November 2018 CPIRP table-top exercise were first completed in December 2020, only after we asked for them. An FHFA official attributed this failure to an oversight.

- Subsequent to circulation of a draft of this report, this FHFA official told us that the CPIRP table-top exercise was not what FHFA used to achieve the goal set out in the Incident Response Standard. This official maintained that FHFA's November 2019 Annual Disaster Recovery Exercise After Action Report (After Action Report) demonstrated that FHFA complied with its Incident Response Standard.

- That After Action Report states, "The purpose of this DR [Disaster Recovery] Exercise is to validate the proper operation of the resiliency and recovery measures incorporated into the overall IT infrastructure. These measures ensure the restoration of the production computing environment within an acceptable period of time in the event of an incident or disaster that disrupts normal computer operations." We found no discussion in this After Action Report of testing performed by FHFA of its incident response capabilities. For that reason, this report does not satisfy FHFA's internal requirement for annual testing of incident response capabilities.

38% of Sampled FHFA Employees and Contractors Did Not Report a Suspicious Phone Call We Made to Test User Compliance with a Requirement in FHFA's Rules of Behavior

As discussed earlier, all users must agree to FHFA's Rules of Behavior prior to gaining access to FHFA information systems and annually reaffirm their agreement with these Rules. Among other things, the Rules require users to immediately report any suspected or potential security incidents, data breaches, or non-compliance with these Rules to OTIM's Help Desk.

We developed a test to check user awareness of and compliance with this requirement in FHFA's Rules of Behavior. That test consisted of a phone call to FHFA users on their FHFA-assigned phones in which we informed the user that certain work information (i.e., name, FHFA phone number, FHFA username, and FHFA password) had been published on the Dark

Web.[11] Prior to the call, FHFA agreed that this call was a reasonable test of employee compliance with this reporting requirement in its Rules of Behavior.[12]

To conduct the test, we called a sample of 120 FHFA users (employees and contractors). We spoke with 5 users and left voice mail for the other 115 users, all on their FHFA-assigned phones, and provided the test message information. From FHFA documentation, we found that 45 FHFA users (38%) we contacted in the test did not report the call or the voice mail to the Help Desk or Information Technology (IT) Security.

FINDINGS

- FHFA did not maintain complete records of security incidents reported to US-CERT, in disregard of its own standard and federal reporting requirements.

[11] The Dark Web is a decentralized network of internet sites that try to make users as anonymous as possible by routing all their communications through multiple servers and encrypting it at each step. Among other things, the Dark Web internet sites facilitate illicit activities, such as trading in stolen accounts and credit cards.

[12] In a technical comment to a draft of this report, FHFA took issue with our statement that its officials agreed that our proposed test call was a reasonable test of employee compliance with the reporting requirement in its Rules of Behavior. For each audit, we develop Rules of Engagement that we discuss with FHFA officials and that FHFA and OIG execute. In drafting Rules of Engagement for this audit, we discussed the proposed test with FHFA officials and this report reflects the agreement reached with those officials.

Within hours of the first test call, the voice mail message that was left on a FHFA phone was forwarded to OTIM. Thereafter, FHFA issued the following notice to all employees, acknowledging that a number of users notified OTIM of this suspicious activity in accordance with the reporting requirement in FHFA's Rules of Behavior:

FHFA OIG Social Engineering Test

As part of an ongoing audit on incident response, the FHFA Office of Inspector General conducted a social engineering test in mid-December. They notified staff that their name, phone number, and FHFA username were available on the dark web. A number of users notified OTIM of this suspicious activity, as stated in the FHFA Information Systems Rules of Behavior. As this was a social engineering test, no further actions were required (except to delete the message). Several users expressed concern about the test, but neither the Help Desk nor OTIM were permitted to respond to users following their inquiries. Thank you to those that reported this activity. Please continue to be vigilant.

FHFA also maintains that its Rules of Behavior do not require all FHFA users to listen to voice mails. That assertion ignores other standards established by FHFA for its employees. While FHFA's Rules of Behavior do not require employees to listen to voice mails, its Telework Policy directs: "Generally, employees are expected to respond within one hour to e-mails and voice mails." At the time we conducted this test, FHFA employees were on mandatory telework due to COVID-19 and FHFA's stated expectation, set forth in its Telework Policy, was that employees would respond to voice mails within an hour.

- FHFA did not contemporaneously document meeting minutes for its November 2018 incident response table-top exercise, as required by its own standard.
- 38% of sampled FHFA employees and contractors failed to follow a reporting requirement in FHFA's Rules of Behavior.

CONCLUSION

Strong incident response controls are necessary to monitor and detect security incidents on a computer or network and to ensure the execution of proper responses to those incidents. While FHFA established and maintained an Incident Response Plan and used its SIEM tool, we found, in this audit, that FHFA did not record, track, or report all security incidents to US-CERT or contemporaneously document the results of a table-top exercise. In addition, 38% of sampled FHFA users did not report a suspicious phone call made to test user compliance with a reporting requirement in FHFA's Rules of Behavior.

RECOMMENDATIONS

We recommend that FHFA:

1. Develop and implement 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.
2. Ensure that minutes documenting future incident response tabletop exercises are prepared timely.
3. Continue to emphasize to employees and contractors the need to report suspicious activities, including phone calls, to the Help Desk in accordance with FHFA's Rules of Behavior.

FHFA COMMENTS AND OIG RESPONSE

OIG provided FHFA an opportunity to respond to a draft of this audit report. FHFA provided technical comments that we incorporated into this final report, as appropriate. On June 2, 2021, FHFA provided its management response, which is provided in the Appendix. In its

response, FHFA disagreed with recommendation 1, and agreed with recommendations 2 and 3. FHFA's comments and our responses are below.

FHFA Comments to Recommendation 1

FHFA disagrees with this recommendation. It asserts that its Incident Response Plan procedure addresses the appropriate information needed and will take no further action.

OIG Response to FHFA Comments to Recommendation 1. As we showed in this report, OTIM lacks written procedures for recording, tracking, or reporting security incidents. FHFA's written response stating that its Incident Response Plan procedure addresses the appropriate information is incorrect.

In a meeting subsequent to the issuance of the final draft of this report, FHFA officials took a different position. They asserted that FHFA has written procedures but acknowledged that those written procedures needed to be enhanced to include the pertinent information that needs to be recorded, tracked, and reported for all security incidents, including those reported to US-CERT, as well as controls to ensure the accuracy and completeness of those records.

However, FHFA's written response is at odds with the verbal statements made by its officials.

We consider this recommendation rejected even though FHFA officials acknowledged orally, the existing procedures are inadequate. We encourage FHFA to enhance its Incidence Response Plan to include written procedures for recording, tracking, and reporting security incidents and develop the commensurate controls to ensure the accuracy and completeness of the security incident records.

FHFA Comments to Recommendation 2

FHFA agrees with this recommendation.

OIG Response to FHFA Comments to Recommendation 2. To the extent that FHFA has committed to ensure that minutes documenting future incident response tabletop exercises are prepared timely, we consider the intent of the recommendation met.

FHFA Comments to Recommendation 3

FHFA agrees with this recommendation and agrees to continue to emphasize to employees and contractors the need to report suspicious activities to the Help Desk in accordance with FHFA's Rules of Behavior.

OIG Response to FHFA Comments to Recommendation 3. To the extent FHFA has committed to continue to emphasize to employees and contractors the need to report suspicious activities, we consider the intent of the recommendation met.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

We conducted this audit to assess FHFA's incident detection and response controls against standards and guidelines established by FHFA and the federal government. Our review period was fiscal years 2019 and 2020.

To accomplish our objective, we:

- Examined FHFA's incident tracking spreadsheet of potential incidents and compared them to incidents reported by the Agency to US-CERT.
- Reviewed the following NIST publications:
  - NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010, updated November 2010)
  - NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013, updated January 2015)
- Reviewed the following FHFA policies, procedures, and related documents:
  - Incident Response Standard, Rev. 1.4, dated May 22, 2020
  - Information Security Incident and Personally Identifiable Information Breach Response Plan, Rev. 4.0, dated August 1, 2019
  - Security Operations Center Strategy, Rev. 1.4, May 28, 2020
  - Information Security Malware Response Procedures, dated June 12, 2019
  - Information System Rules of Behavior and User Acknowledgement, FHFA Form #050, dated October 2018.
- Reviewed and analyzed FHFA's Incident Response Plan and determined whether the plan included preparation, detection and analysis, containment, eradication and recovery. Also determined whether FHFA's management approved the plan and communicated the plan and any updates to all personnel with incident response responsibilities.

- Reviewed and analyzed FHFA's incident response training records, and determined whether training was provided to members of the incident response team and Help Desk staff within one year of assuming an incident response role or responsibility, when required by information system changes, and annually thereafter.

- Reviewed and analyzed FHFA's incident response test plan and results, and determined whether FHFA tested incident response capabilities annually using pre-defined tests to determine incident response effectiveness and documented the results.

- Assessed FHFA's incident detection and response controls using the *Standards for Internal Control in the Federal Government*.[13] We determined that the control activities component of internal control was significant to our objective, along with the underlying principle that management should design control activities to achieve objectives and respond to risks.

- Developed and conducted a test to check employees' and contractors' awareness of and compliance with FHFA's Rules of Behavior. We called and either spoke with or left a voice mail for a random sample of 120 FHFA employees and contractors. The random sample was selected from a list of 591 employees and contractors that we collected from FHFA's internal phone directory.

- Interviewed officials, staff, and contractors of FHFA's OTIM regarding FHFA's policies, procedures, and process for incident response.

We conducted this performance audit between October 2020 and June 2021 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 objective.

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

APPENDIX: FHFA MANAGEMENT RESPONSE.....

Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Senior Audit Executive

FROM: Kevin Smith, Chief Information Officer KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2021.06.24 09:27:24 -04'00'

SUBJECT: Draft Audit Report: FHFA Did Not Record, Track, or Report All Security Incidents to US-CERT; 38 % of Sampled FHFA's Users Did Not Report a Suspicious Phone Call Made to Test User Awareness of its Rules of Behavior

DATE: June 2, 2021

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

Recommendation 1: *Develop and implement 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.*

Management Response: FHFA disagrees with Recommendation 1, as FHFA's Information Security Incident and PII Information Breach Response Plan (Plan) procedure addresses the appropriate information needed and will take no further action. Based on the US CERT Guidance dated April 1, 2017, FHFA was not required to report the lost encrypted iPhones or Laptops nor had any reportable events in Fiscal Years 2019 or 2020. If FHFA does have a US CERT reportable event, it will track the corresponding US CERT number in its system of record, per the existing procedure.

Recommendation 2: *Ensure that minutes documenting future incident response tabletop exercises are prepared timely.*

Management Response: FHFA agrees with Recommendation 2, however, FHFA did not fail to document the meeting minutes in accordance with FHFA's Incident Response Standard as the Cybersecurity Privacy & Incident Response Program (CPIRP) does not fall under the jurisdiction of the Incident Response Standard as Section 1.2, states: "This standard is intended for use by employees and contractors within the OTIM or individuals with specialized roles supporting IT resources." The CPIRP supports FHFA Offices and Divisions that do not have specialized roles supporting IT resources. FHFA's policies and procedures address this recommendation, therefore, and will take no further action.

Recommendation 3: *Continue to emphasize to employees and contractors the need to report suspicious activities, including phone calls, to the Help Desk in accordance with FHFA's Rules of Behavior.*

Management Response: FHFA agrees with Recommendation 3 and agrees to continue to emphasize to employees and contractors the need to report suspicious activities to the Help Desk in accordance with FHFA's Rules of Behavior. Currently, FHFA requires that every FHFA employee and contractor complete the annual Information Security and Privacy Training (Training). The 2021 Training includes topics that employees and contractors should report suspected suspicious activity or breaches to either Information Security or the Help Desk. FHFA expects its employees and contractors to determine if a phone call or email is SPAM and to determine if the SPAM should be reported to Information Security or to the Help Desk. FHFA's annual security training addresses this recommendation and will not take any further action.

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

CC: Chris Bosland
Kate Fulton
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