Federal Housing Finance Agency
Office of Inspector General

FHFA Did Not Fully Comply with DHS Binding Operational Directives for Securing Its Public Websites and Publishing Its Vulnerability Disclosure Policy

Audit Report • AUD-2022-010 • August 31, 2022

AUD-2022-010

August 31, 2022

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency) is charged by the Housing and Economic Recovery Act of 2008 with the supervision of Fannie Mae and Freddie Mac (together, the Enterprises); Common Securitization Solutions, LLC (an affiliate of each Enterprise); the Federal Home Loan Banks; and the Federal Home Loan Banks' fiscal agent, the Office of Finance (collectively, the regulated entities). FHFA's mission is to ensure the safety and soundness of its regulated entities so that they serve as a reliable source of liquidity and funding for housing finance and community investment. Since September 2008, FHFA has also served as conservator for the Enterprises.

Pursuant to the Federal Information Security Modernization Act of 2014 (FISMA), Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives (BODs). A BOD is a compulsory directive to federal executive branch departments and agencies for purposes of safeguarding federal information and information systems. Federal agencies are required to comply with DHS-developed directives.

We conducted this audit to determine whether FHFA complied with select DHS BODs. Our review period was October 1, 2020, through September 30, 2021 (review period). We selected DHS BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*; DHS BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*; and DHS BOD 18-01, *Enhance Email and Web Security* because each BOD required ongoing actions to be taken by the Agency during the review period.

We found that FHFA complied with DHS BOD 19-02 requirements. However, contrary to DHS BOD 18-01, FHFA did not configure all of its publicly accessible websites and web services with a secured connection because these websites and web services were managed by a third-party vendor and were not under FHFA's control. Unsecured connection to these websites and web services could subject user information to interception, eavesdropping, tracking, and modification. FHFA also did not include an issuance date in its Vulnerability Disclosure Policy (VDP), which DHS BOD 20-01 requires, due to an oversight. Without the issuance date of the VDP, the public cannot determine if the policy is up to date. Finally, FHFA did not develop and maintain documented policies and procedures governing the process of implementing DHS BODs because the Chief Information Security Officer (CISO) relies on an informal undocumented process. Without documented policies and procedures, FHFA may respond to DHS BODs in an ad-hoc, reactive manner.

AUD-2022-010

August 31, 2022

We make three 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; David Peppers, Auditor-in-Charge; Zachary Lewkowicz, IT Auditor; 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

BOD	Binding Operational Directive
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DMARC	Domain-based Message Authentication, Reporting, and Conformance
Enterprises	Fannie Mae and Freddie Mac
FHFA or Agency	Federal Housing Finance Agency
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HSTS	HTTP Strict Transport Security
IP	Internet Protocol
OMB	Office of Management and Budget
OTIM	Office of Technology and Information Management
Regulated Entities	Fannie Mae, Freddie Mac, any affiliate of Fannie Mae and Freddie Mac, and the Federal Home Loan Banks
SSL	Secure Sockets Layer
VDP	Vulnerability Disclosure Policy

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 general support system provides connectivity between the Agency's sites, headquarters, and data centers, internet access, email, and directory services for all agency divisions and offices.

FHFA's Office of Technology and Information Management (OTIM) works with mission and support offices to promote the effective and secure use of information and systems.

Department of Homeland Security Binding Operational Directives

The Cybersecurity and Infrastructure Security Agency (CISA), an operational component under DHS, develops and oversees the implementation of BODs, which require action on the part of certain federal agencies in the civilian Executive Branch. These directives require agencies to complete required actions to protect federal information and information systems from known information security threats, vulnerabilities, and risks. Since 2015, DHS has issued ten BODs that instruct agencies to, among other things, (1) publish and maintain a vulnerability disclosure policy on an agency's public website, (2) remediate critical and high vulnerabilities discovered by DHS through its scanning of agencies' internet-accessible systems, and (3) ensure that publicly accessible websites[1] and web services[2] (hereafter referred to as "websites") provide service only through a secure connection.

DHS BOD 20-01—Develop and Publish a Vulnerability Disclosure Policy (September 2, 2020)

In 2020, Office of Management and Budget (OMB) issued memorandum M-20-32, "Improving Vulnerability Identification, Management, and Remediation" (September 2020), providing federal agencies with guidance for obtaining and managing their vulnerability research programs. DHS BOD 20-01 was issued in support of OMB M-20-32, which requires each agency to develop a Vulnerability Disclosure Policy (VDP)[3] and publish it on its public

[1] A website is 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.

[2] A web service is a software component or system designed to support machine or application interactions over a network. A web service also has an interface that can interact with a computer or other systems.

[3] A VDP establishes processes and procedures for the security research community to report vulnerabilities to appropriate agency contacts, who can then use the reports to address vulnerabilities of which they may not

website. The VDP must include the systems in scope, the types of testing that are allowed, a description of how to submit vulnerability reports, a commitment to not recommend or pursue legal action, a statement with expectations for acknowledgement of the reporter, and an issuance date. Figure 1 outlines actions for developing and publishing a VDP.

FIGURE 1. DHS BOD 20-01 REQUIREMENTS

Timeline	Directive Requirements
By October 2, 2020*	Update the "Security Contact" field for each .gov domain registered on the .gov Registrar.[4] Update the "Organization" field for each .gov domain registered on the .gov Registrar.
By March 1, 2021*	Publish a VDP as a public web page at the "/vulnerability-disclosure-policy" path of the agency's primary .gov website. After publication of the VDP, immediately report any newly discovered vulnerabilities to CISA or any vulnerability disclosure, coordination, or remediation activities where CISA can assist. Develop or update vulnerability disclosure handling procedures to support the implementation of the VDP.
By May 30, 2021, and within every 90 days thereafter*	The scope of the VDP must increase by at least one internet-accessible system or service until all systems and services are in scope of the policy.
By May 30, 2021, and quarterly thereafter*	Report metrics on vulnerability disclosure reports through CyberScope.[5]
By September 2, 2022*	All internet-accessible systems or services must be in the scope of the policy.

Source: FHFA-OIG analysis of DHS BOD 20-01 *Develop and Publish a Vulnerability Disclosure Policy*.

* These requirements are ongoing for the agencies to ensure compliance for VDP published on public websites.

have been aware. A VDP makes it easier for the public to know what types of testing are authorized for which systems, what communication to expect, and where to send a report.

[4] The .gov Registrar is a website managed by CISA for registration of .gov domains.

[5] CyberScope is the platform for the FISMA reporting process. Chief Information Officers, Inspectors General, and Senior Agency Officials for Privacy as well as micro agencies all report through CyberScope.

DHS BOD 19-02—Vulnerability Remediation Requirements for Internet-Accessible Systems (April 29, 2019)

Federal agencies operate interconnected and complex systems that expand their internet presence through increased deployment of internet-accessible systems. This makes it more critical than ever to rapidly remediate vulnerabilities that could allow malicious actors to compromise these systems. CISA operates a Cyber Hygiene scanning service[6] that reports on vulnerabilities of all severities[7] in weekly reports sent to agencies. DHS BOD 19-02 provides a federal cybersecurity standard for remediating critical and high vulnerabilities. As such, agencies are responsible for managing and prioritizing cybersecurity risk appropriately within their environments. DHS BOD 19-02 requires agencies to remediate critical[8] and high[9] vulnerabilities by required timeframes and report to CISA if the vulnerabilities are not remediated within the specified timelines. Figure 2 outlines remediation timeline and reporting requirements.

FIGURE 2. DHS BOD 19-02 REQUIREMENTS

Timeline	Directive Requirements
After issuance date (April 29, 2019)	Ensure Cyber Hygiene scanning access by removing Cyber Hygiene source IP addresses from block lists.
Within 5 working days of change to an agency's internet-accessible Internet Protocol (IP) addresses*	Notify CISA of modifications.

[6] Cyber Hygiene leverages the Common Vulnerability Scoring System (CVSS), which is a vulnerability scoring system designed to provide a universally open and standardized method for rating information technology vulnerabilities.

[7] Vulnerabilities are based upon a CVSS v3.0 score that helps organizations prioritize vulnerability management strategies by providing a score representative of the base, temporal, and environmental properties of a vulnerability. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS v3.0 score is also represented as a vector string, a compressed textual representation of the values used to derive the score. See table below.

Vulnerability	Low	Medium	High	Critical
Base Score	0.1-3.9	4.0-6.9	7.0-8.9	9.0-10.0

[8] See footnote 7.

[9] See footnote 7.

Timeline	Directive Requirements
Within 15 calendar days of initial detection*	Review Cyber Hygiene reports by CISA and remediate the critical vulnerabilities.
Within 30 calendar days of initial detection*	Review Cyber Hygiene reports by CISA and remediate the high vulnerabilities.

Source: FHFA-OIG analysis of DHS BOD 19-02 *Vulnerability Remediation Requirements for Internet-Accessible Systems*.

* These requirements are ongoing required actions for the agencies to ensure timely remediation of critical and high vulnerabilities after they were detected.

DHS BOD 18-01—Enhance Email and Web Security (October 16, 2017)

DHS BOD 18-01 directs agencies to implement specific security standards to strengthen email authentication and web security by a required timeline.

Email Security

DHS BOD 18-01 requires agencies to enable STARTTLS[10] and improve email authentication by implementing a Domain-based Message Authentication, Reporting, and Conformance (DMARC)[11] policy to reduce the risk of attacks from unauthorized email senders. In addition, CISA provides Cyber Hygiene Assessment Trustworthy Email Reports that measure the presence of DMARC records on an agency's internet-facing mail servers, as well as support for STARTTLS. CISA provides weekly reports to help agencies comply with the email security aspects of DHS BOD 18-01. Figure 3 outlines actions for implementing email security requirements.

[10] STARTTLS is a command for upgrading a previously insecure internet connection to a secure connection. When enabled by a receiving mail server, STARTTLS signals to a sending mail server that the capability to encrypt an email in transit is present. Enabling STARTTLS makes passive man-in-the-middle attacks more difficult.

[11] DMARC is a proposed standard that allows email senders and receivers to cooperate in sharing information about the email they send to each other. This information helps senders improve the mail authentication infrastructure so that all their mail can be authenticated. It also gives the legitimate owner of an internet domain a way to request that illegitimate messages – spoofed spam, phishing – be put directly in the spam folder or rejected outright.

FIGURE 3. DHS BOD 18-01 EMAIL SECURITY REQUIREMENTS

Timelines	Directive Requirements
By November 16, 2017	Develop and provide to DHS an "Agency Plan of Action for BOD 18-01" and begin implementing the plan.
By December 15, 2017*	Provide a report to DHS on the status of that implementation and continue to report every 30 calendar days thereafter until implementation of the agency's BOD 18-01 plan is complete.
By January 15, 2018*	Configure all internet-facing mail servers to offer STARTTLS, which makes passive man-in-the-middle attacks[12] more difficult. Improve email authentication by implementing DMARC policy, which reduces the risk of attacks from unauthorized email senders.
By February 13, 2018*	Disable Secure Sockets Layer (SSL)[13] versions 2 and 3 on mail servers, which had been disapproved and were replaced by a newer version of SSL because of known security vulnerabilities. Disable weak encryption standards 3DES[14] and RC4[15] on mail servers.
Within 15 days (of the establishment of a centralized National Cybersecurity & Communications Integrations Center reporting location)*	Add reports@dmarc.cyber.dhs.gov as a recipient of DMARC aggregate reports.
By October 16, 2018*	Configure a DMARC policy of "reject" for all second-level domains and mail-sending hosts to block delivery of unauthenticated messages.

Source: FHFA-OIG analysis of DHS BOD 18-01 *Enhance Email and Web Security*.

* These requirements are ongoing for the agencies to ensure email security for current internet-facing mail servers.

[12] A man-in-the-middle attack is where an attacker is positioned between two communicating parties in order to intercept or alter data traveling between them.

[13] Secure Sockets Layer (SSL) provides privacy and data integrity between two communicating applications. It is designed to encapsulate other protocols, such as HTTP. The protocol is composed of two layers: the Transport Layer Security (TLS) record protocol and the TLS handshake protocol. Deprecated SSL means a version of SSL has been disapproved and replaced by a newer version of SSL because of known security vulnerabilities.

[14] 3DES is an implementation of the data encryption standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than the advanced encryption standard (AES).

[15] Rivest Cipher 4, or RC4, is a stream cipher created in 1987. A stream cipher is a type of cipher that operates on data a byte at a time to encrypt that data. A flaw was found in RC4 where the encryption key used by RC4 could be cracked and obtained in less than a minute.

Web Security

In 2015, OMB issued memorandum M-15-13, "A Policy to Require Secure Connections across Federal Websites and Web Services" (June 2015), requiring all publicly accessible federal websites and web services to enforce the use of Hypertext Transfer Protocol Secure (HTTPS)[16] and HTTP Strict Transport Security (HSTS).[17] Additionally, DHS BOD 18-01 requires that agencies remove known weak encryption protocols (SSLv2 and SSLv3) and encryption standards (RC4 and 3DES). CISA provides Cyber Hygiene Assessment HTTPS Reports on vulnerabilities of all severities in weekly Cyber Hygiene reports sent to agencies. CISA provides these reports to help agencies comply with the web security aspects of DHS BOD 18-01. Figure 4 outlines actions for implementing web security requirements.

FIGURE 4. DHS BOD 18-01 WEB SECURITY REQUIREMENTS

Timeline	Directive Requirements
By November 16, 2017	Develop and provide to DHS an "Agency Plan of Action for BOD 18-01" and begin implementing the plan.
By December 15, 2017*	Provide a report to DHS on the status of that implementation and continue to report every 30 calendar days thereafter until implementation of the agency's BOD 18-01 plan is complete.
By February 13, 2018*	Configure all publicly accessible websites with secure connection (HTTPS-only, with HSTS). Disable SSL versions 2 and 3 on web servers, which had been disapproved and were replaced by a newer version of SSL because of known security vulnerabilities. Disable weak encryption standards, 3DES and RC4, on web servers. Identify and provide a list to DHS of agency second-level domains that can be HSTS preloaded, which will enforce the use of HTTPS for all subdomains and allows agencies to avoid inventorying and configuring an HSTS policy for every individual subdomain.

Source: FHFA-OIG analysis of DHS BOD 18-01 *Enhance Email and Web Security*.

* These requirements are ongoing for agencies to ensure secured connection for publicly accessible websites.

[16] HTTP is a standard method for communication between clients and web servers. HTTPS verifies the identity of a website or web service for a connecting client and encrypts nearly all information sent between the website or service and the user.

[17] HTTP Strict Transport Security (HSTS) instructs compliant browsers to assume HTTPS going forward. This reduces insecure redirects and protects users against attacks that attempt to downgrade connections to plain HTTP.

FACTS AND ANALYSIS

FHFA Complied with DHS BOD 19-02 Requirements

As required by DHS BOD 19-02, we found that FHFA:

- Provided access to CISA for Cyber Hygiene scanning of its internet-accessible systems.
- Did not have any critical or high vulnerabilities reported by CISA that required remediation.

FHFA Did Not Fully Comply with DHS BODs for Securing Its Publicly Accessible Websites and Publishing Its Vulnerability Disclosure Policy

Contrary to DHS BOD 18-01, FHFA Did Not Configure All of Its Publicly Accessible Websites with Secured Connection

Although FHFA complied with BOD 18-01 email security requirements, FHFA did not fully comply with all web security requirements. According to DHS Cyber Hygiene Assessment HTTPS Report, dated September 25, 2021, FHFA did not configure 4[18] of its 43 (9.3%) publicly accessible websites with HTTPS. During our audit, we tested and determined that 6[19] of 43 publicly accessible websites (14%) were not configured with HTTPS and were utilizing an unencrypted HTTP protocol.

The unencrypted HTTP protocol does not protect data from interception or alteration, which can subject users to unsecured eavesdropping, tracking, and the modification of received data. HTTP connections can be easily monitored, modified, and impersonated. HTTPS is designed to prevent this information from being read or changed while in transit. HTTPS verifies the

[18] In February 2022, consistent with the guidance in DHS Cyber Hygiene Assessment HTTPS Report, FHFA excluded 3 of 4 publicly accessible websites from the BOD 18-01 requirements for HTTPS because these websites are used for Online Certificate Status Protocol (OCSP). OCSP provides services to verify if a website is using HTTPS. OTIM officials stated the 1 remaining publicly accessible website was a false positive and contacted CISA for guidance in June 2022. On July 1, 2022, CISA informed FHFA that there are known challenges with bringing the 1 remaining publicly accessible website into compliance because a third-party vendor would need to update the website to make it compliant. CISA also provided workarounds that included contacting the third-party vendor to explore a solution, which worked for another agency.

[19] This includes the 4 of 43 websites initially reported by DHS and an additional 2 of 43 publicly accessible FHFA websites. FHFA stated that the 2 websites were not configured with HTTPS because they were managed by the same third-party vendor and not under FHFA's control.

identity of a website for a connecting client and encrypts information sent between the website and the user.

Additionally, the DHS Cyber Hygiene Assessment HTTPS Report stated that FHFA did not configure 17[20] of 43 websites (39.5%) with HSTS requirements. We tested and determined that FHFA still has not configured 5[21] of 43 websites (11.6%) with HSTS.

OTIM officials stated that they did not configure all FHFA publicly accessible websites with secured connections as required by the BOD because these websites were managed by a third-party vendor and were not under FHFA's control. Additionally, they stated there is nothing more that FHFA could do about these configurations. CISA has provided potential workarounds that included contacting the third-party vendor to explore a solution, which worked for another agency.

By FHFA not configuring its publicly accessible websites with secured connections, FHFA is in noncompliance with the BOD 18-01 requirements for web security. Unsecured connection to these websites could subject user information to interception, eavesdropping, tracking, and modification. Further, FHFA's systems connecting to these websites with unencrypted protocols could be compromised from potential man-in-the-middle attacks that may also lead to additional vulnerabilities in FHFA systems.

FHFA Did Not Include One Required Element in Its Vulnerability Disclosure Policy Published on Its Public Website, as required by DHS BOD 20-01

Although FHFA developed a VDP and published it on its public website, FHFA did not include one of the BOD 20-01 required elements in its VDP. Specifically, FHFA did not include the issuance date for the VDP. FHFA officials stated that the issuance date was not included in the VDP due to an oversight. By not including the issuance date in the VDP, FHFA is in noncompliance with BOD 20-01. Without the issuance date of the VDP, the public cannot determine if the policy is up to date.

---

[20] In September 2021, FHFA could not configure 12 of 17 publicly accessible websites. OTIM officials could not recall the reason these websites were not configured securely. In November 2021, FHFA decommissioned these websites. In February 2022, consistent with the guidance in DHS Cyber Hygiene Assessment HTTPS Report, FHFA excluded 3 of 17 publicly accessible websites from the BOD 18-01 requirements for HSTS because these websites are used for Online Certificate Status Protocol (OCSP). OCSP provides services to verify if a website is using HTTPS. OTIM officials stated the 2 remaining publicly accessible websites were a false positive and contacted CISA for guidance in June 2022. On July 1, 2022, CISA informed FHFA that there are known challenges with bringing the 2 remaining publicly accessible websites into compliance because a third-party vendor would need to update the website to make it compliant. CISA also provided workarounds that included contacting the third-party vendor to explore a solution, which worked for another agency.

[21] All 5 websites were part of the 17 websites initially reported by DHS.

FHFA Did Not Develop and Maintain Documented Policies and Procedures Governing the Process of Implementing DHS BODs

FHFA did not develop and maintain documented policies and procedures to guide the process of implementing DHS BODs.[22] According to the CISO, he and his team receive DHS BODs through different distribution lists, and he assigns it to the appropriate analyst for processing. The CISO said there is no formal documented process. Without documented policies and procedures, FHFA may respond to DHS BODs in an ad-hoc, reactive manner. For example, in the absence of the CISO, OTIM staff may not have defined responsibilities for handling the BODs, and the required actions may not be completed timely in response to DHS BODs.

FINDINGS

- Contrary to DHS BOD 18-01, FHFA did not configure all of its publicly accessible websites with a secured connection because, according to FHFA, these websites were managed by a third-party vendor and were not under FHFA's control.
- FHFA did not include one required element in its VDP published on its public website due to an oversight.
- FHFA did not develop and maintain documented policies and procedures governing the process of implementing DHS BODs, choosing instead to rely on an informal undocumented process.

CONCLUSIONS

FHFA is required to comply with DHS BODs for the purposes of safeguarding federal information and information systems. We conclude that FHFA complied with some, but not all, DHS BODs reviewed as a part of this audit. Our three recommendations are designed to help mitigate the cyber risks posed by noncompliance with the BODs.

[22] *Standards for Internal Control in the Federal Government* (Green Book) state 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.

RECOMMENDATIONS

We recommend that the Chief Information Officer at FHFA:

1. Identify and implement a solution, in coordination with vendors, for meeting BOD 18-01 requirements to ensure all publicly accessible endpoints provide service through a secure connection (HTTPS-only, with HSTS). If there are no viable solutions, document any risk-based decisions, including compensating controls, for publicly accessible websites that are not in compliance with DHS BOD 18-01.

2. Update the VDP published on FHFA's public website to include an issuance date.

3. Develop and maintain policies and procedures for implementing DHS BODs.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA an opportunity to respond to a draft of this audit report. FHFA provided technical comments on the draft report and those comments were considered in finalizing this report. FHFA also provided a management response, which is included in the Appendix to this report. In its management response, FHFA agreed with our recommendations and included the following planned corrective actions:

1. FHFA has remediated two of the three identified weaknesses. FHFA will work with the vendor to remediate the third weakness. If a remediation is not available, FHFA will develop a risk or a closure memorandum by July 31, 2023.

2. FHFA updated the VDP on its public website to include an issuance date on July 25, 2022. FHFA will take no further action on Recommendation 2 but will submit a closure memorandum by October 31, 2022.

3. FHFA will document a high-level procedure by December 31, 2022.

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 complied with select DHS BODs. We selected DHS BOD 20-01, DHS BOD 19-02, and DHS BOD 18-01 due to their ongoing required actions needing to be taken by the Agency. Our review period was October 1, 2020, through September 30, 2021.

To accomplish our objective, we:

- Reviewed Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G (September 2014), and determined that the control activities component of internal control was significant to this objective, focusing on the underlying principle that management should design the entity's information system and related control activities to achieve objectives and respond to risks, and implement control activities through policies.

- Reviewed and completed an analysis of the following BODs:

    - BOD 20-01 – *Develop and Publish a Vulnerability Disclosure Policy*

- BOD 19-02 – *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- BOD 18-02 – *Securing High Value Assets*
- BOD 18-01 – *Enhance Email and Web Security*
- BOD 17-01 – *Removal of Kaspersky-branded Products*
- BOD 16-03 – *2016 Agency Cybersecurity Reporting Requirements*
- BOD 16-02 – *Threat to Network Infrastructure Devices*
- BOD 16-01 – *Securing High Value Assets*
- BOD 15-01 – *Critical Vulnerability Mitigation*

- Excluded BODs 16-01 and 15-01 from our scope because they were revoked.
- For BODs 17-01 and 16-03 determined there were no required actions to be taken during the review period.
- For BODs 18-02 and 16-02, determined that FHFA had no further actions required as it had already completed the requirements in the BODs.
- Selected the following BODs for testing: 20-01, 19-02, and 18-01 for this audit due to their ongoing required actions required by the agency during the review period.
- Determined whether FHFA complied with and completed the required actions as directed by DHS BOD 20-01 and retained records of required information submitted to DHS. Specifically, we reviewed and analyzed:
  - The .gov Registrar to determine if FHFA updated the security contact and organization fields for the fhfa.gov and harp.gov domains.
  - FHFA's vulnerability disclosure policy.
  - FHFA's vulnerability disclosure procedures.
  - FHFA's vulnerability disclosure reporting metrics reports.
- Determined whether FHFA completed the required actions as directed by DHS BOD 19-02 and retained records of required information submitted to DHS. Specifically, we obtained, reviewed, and analyzed CISA's Cyber Hygiene reports issued to FHFA

for critical and high vulnerabilities detected on the Agency's internet-accessible systems.

- Determined whether FHFA complied with required actions as directed by DHS BOD 18-01 and retained records of required information submitted to DHS. Specifically, we:
  - Obtained, reviewed, and analyzed FHFA's plan of action for BOD 18-01.
  - Obtained, reviewed, and analyzed Cyber Hygiene Assessment Trustworthy Email Reports and HTTPS Reports issued by CISA to FHFA regarding the Agency's compliance with BOD 18-01's email and web security requirements.
  - Obtained, reviewed, and analyzed FHFA's DMARC aggregate reports.
  - Tested 43 of FHFA's publicly accessible websites to determine if they were configured with HTTPS and HSTS. Also, tested these websites to determine if deprecated encryption protocols SSL version 2 and version 3 and encryption cyphers 3DES and RC4 were not in use.
  - Tested FHFA's internet-facing mail servers to determine if deprecated encryption protocols SSL version 2 and version 3 and encryption cyphers 3DES and RC4 were not in use.
- Interviewed OTIM officials, staff, and contractors regarding the Agency's compliance with the selected BODs.

We conducted this performance audit between October 2021 and August 2022 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.....

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: 2022.08.19 14:49:19 -04'00'

FROM: Jason Donaldson, Acting Chief Information Officer JASON DONALDSON Digitally signed by JASON DONALDSON Date: 2022.08.19 13:48:29 -04'00'

SUBJECT: Draft Audit Report: FHFA Did Not Fully Comply with DHS Binding Operational Directives for Securing its Public Websites and Publishing its Vulnerability Disclosure Policy

DATE: August 17, 2022

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

Recommendation 1: *Identify and implement a solution, in coordination with vendors, for meeting BOD 18-01 requirements to ensure all publicly accessible websites provide service through a secure connection (HTTPS-only, with HSTS) or document any risk-based decisions if there is not a viable solution to make all websites compliant.*

Management Response: FHFA agrees with Recommendation 1. FHFA has remediated two of the three identified weaknesses. FHFA will work with the vendor to remediate the third weakness. If a remediation is not available, FHFA will develop a risk or a closure memo by July 31, 2023.

Recommendation 2: *Update the VDP published on FHFA's public website to include an issuance date.*

Management Response: FHFA agrees with Recommendation 2. FHFA updated the VDP on its public website to include an issuance date on July 25, 2022. FHFA will take no further action on Recommendation 2 but will submit a closure memo by October 31, 2022.

Recommendation 3: Develop and maintain policies and procedures for implementing DHS BODs.

Management Response: FHFA agrees with Recommendation 3. FHFA will document a high-level procedure by December 31, 2022.

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

cc: Edom Aweke
Tom Leach
Tasha Cooper
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