Federal Housing Finance Agency
Office of Inspector General

Vulnerabilities in FHFA's Public-Facing Systems Risk Unauthorized Access to Non-Public Data

Audit Report • AUD-2025-007 • September 25, 2025

.... EXECUTIVE SUMMARY ....

PURPOSE

As part of our ongoing oversight of the Federal Housing Finance Agency's (FHFA or Agency) compliance with the Federal Information Security Modernization Act (FISMA), we perform audits of networks and information security of the Agency. Our objective for this audit was to determine whether the Agency's security controls were effective to protect its network and systems against external threats and prevent unauthorized access to FHFA's non-public data from January 2025 through July 2025.

RESULTS

We determined that FHFA's security controls were not fully effective to protect its network and systems against external threats. While the Agency successfully blocked simulated email phishing attacks during our social engineering testing, we were able to access its Community Support Program (CSP) website using various institutional identifiers and download internal files without authentication or detection. The CSP website handles personally identifiable information (PII) and operated with incomplete security and privacy documentation. We also found that FHFA's internal video surveillance system (CCTV) was publicly accessible online, unmonitored, and contained known vulnerabilities dating back to 2019.

These vulnerabilities make FHFA's IT infrastructure, and the non-public information stored on it, more susceptible to unauthorized access and security compromises. The scope, severity, and potential impact of these security vulnerabilities are serious matters that require immediate corrective action by FHFA management. Accordingly, we are reporting four findings related to the identified control deficiencies.

RECOMMENDATIONS

We made 19 recommendations to address our findings. In a written response, FHFA management agreed with each of our recommendations.

This report was prepared by Zachary Lewkowicz, IT Audit Manager; Shedaun Smith, IT Specialist; Brian Prisbe, IT Specialist; and Robert Todora, IT Specialist; 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

API	Application Programming Interface
ATO	Authority to Operate
CCTV	Closed Circuit Television
CSP	Community Support Program
CUI	Controlled Unclassified Information
Enterprises	Fannie Mae and Freddie Mac
FHFA or Agency	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Federal Housing Finance Agency Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SP	Special Publication
SSPP	System Security and Privacy Plan
URL	Uniform Resource Locator

BACKGROUND ....

Federal Standards for Information Security

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

FHFA's Network and System

FHFA's Office of the Chief Information Officer (OCIO) works with all FHFA mission and support offices to promote the effective and secure use of information and systems. OCIO's principal responsibilities and functions include:

- Developing an enterprise-wide approach to IT management and governance;
- Ensuring FHFA maintains and enhances a secure computing environment;
- Promoting records and information management;
- Driving innovation; and
- Enhancing Agency-wide business partnerships with other FHFA offices.

FHFA's network and systems host a variety of data and information such as financial reports and data from Fannie Mae and Freddie Mac (the Enterprises), U.S. Financial Technology LLC (formerly known as Common Securitization Solutions, LLC), the Federal Home Loan Banks, and the Office of Finance, as well as FHFA employees' PII. As such, it is important that the configurations and controls in place are effective to prevent unauthorized access to systems and information. If unauthorized access to FHFA's network is successful, attackers may have opportunities to compromise the confidentiality, integrity, and availability of FHFA's non-public information. For example, attackers could extract, delete, or modify this data, including PII; discover usernames and passwords; and launch denial-of-service attacks.[1] If these unauthorized

[1] NIST defines a denial-of-service (DOS) as the prevention of authorized access to a system resource or the delaying of system operations and functions.

activities are not timely detected or prevented, such activities could result in compromises of systems and information, hindering FHFA's mission. To protect against these vulnerabilities, FHFA has implemented a security program that includes security testing and assessments for determining the effectiveness of security controls in safeguarding its information systems and controlled unclassified information (CUI).[2]

OBJECTIVE AND SCOPE ....

The objective of our audit was to determine whether FHFA's security controls protect its network and systems against external threats[3] and prevent unauthorized access to FHFA's non-public data. The audit scope covered FHFA's public-facing information systems from January 2025 through July 2025. This work supports the annual FISMA evaluation of the FHFA's security program and practices.

RESULTS ....

We performed external penetration testing[4] of FHFA's 64 internet-accessible information systems, including 22 public websites, to determine whether the Agency's security controls were effective to protect its network and systems against external threats and prevent unauthorized access to FHFA's non-public data. We determined that FHFA's security controls were not fully effective. While FHFA successfully blocked simulated email phishing attacks during our social engineering testing and demonstrated some effective safeguards, we identified serious security vulnerabilities in other areas during our external penetration testing.

[2] NIST defines CUI as information required by law, regulation, or government-wide policy to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information (December 29, 2009), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

[3] An external threat or outside(r) threat is an unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, or denial of service.

[4] Penetration testing involves assessors mimicking real-world attacks to identify methods for circumventing the security features of an application, system, or network. This type of testing can involve launching actual attacks on live systems and data, using tools and techniques common among attackers. Penetration tests typically look for combinations of vulnerabilities on one or more systems. This approach allows testers to gain more extensive access than they would by targeting a single vulnerability. External penetration testing is conducted from outside the organization's security perimeter. This testing enables the tester to view the security features of an application, system, or network as they appear outside the security perimeter—usually as seen from the internet—with the goal of revealing vulnerabilities that could be exploited by external attackers.

For example, we were able to use various institutional identifiers to login to the CSP[5] website as member banks. Additionally, we were able to exfiltrate non-public data from FHFA's internal network without authentication or detection. The CSP website is designated as a privacy system, meaning it is intended to collect, store, or process PII[6] and must meet elevated privacy and security requirements. Despite this, the system lacked fundamental safeguards such as user authentication, access control, and system monitoring. Notwithstanding these shortcomings, FHFA authorized it to operate with incomplete and inaccurate security and privacy documentation. This documentation did not identify signficant access control risks. Furthermore, FHFA's internal surveillance system (hereinafter referred to as the "CCTV[7] website"), was publicly accessible, contained longstanding vulnerabilities dating back to 2019, and was not being monitored by FHFA.

These vulnerabilities make FHFA's information technology infrastructure and its non-public data more susceptible to unauthorized access and security breaches. We view the scope, severity, and potential impact of these network security vulnerabilities as serious matters that require immediate corrective action from FHFA management. In all, we are reporting four findings:

1. FHFA's CSP website allowed unauthenticated access to internal files, including non-public information.

2. FHFA approved CSP system for use without complete or accurate security documentation.

3. FHFA's privacy impact assessment did not identify risks posed by external CSP users.

4. FHFA's CCTV website was publicly accessible and contained security flaws.

Collectively, these findings reveal that FHFA operated systems without fully understanding their vulnerabilities to unauthorized access, or how to protect them. These lapses allowed our auditors

[5] The Federal Home Loan Bank Act [12 U.S.C. § 1430(g)] requires the FHFA to establish a Community Support Program for members of the Federal Home Loan Banks. Community Support Program regulations [12 C.F.R. part 1290] set forth standards of community investment or service for members of Federal Home Loan Banks to maintain continued access to long-term advances and to community investment products (i.e., Affordable Housing Program and other Community Investment Cash Advances programs). In addition, the regulation sets forth the process that FHFA follows in reviewing, evaluating, and communicating each member's Community Support performance

[6] The CSP system collects, uses, disseminates, or maintains information such as the Bank members' senior officers' (submitter) name, work title, and business email, which is all set forth in the Community Support Statement (060 Form); Bank members' contact information; data on their Community Reinvestment Act of 1977 performance, if applicable; and data on members' compliance with the First Time Homebuyer requirement.

[7] Closed Circuit Television is a video surveillance system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

to obtain unauthorized access to non-public data and systems during testing. If a malicious actor had conducted this as a real-world attack, FHFA's mission, operations, and public trust could have suffered significant harm.

Finding 1: FHFA's CSP Website Allowed Unauthenticated Access to Internal Files, Including Non-public Information

FHFA's public CSP website exposed internal FHFA files and data of the member banks of the Federal Home Loan Bank System (hereinafter referred to as member banks)[8] to anyone on the internet without requiring authentication. We found that by modifying the website's uniform resource locator (URL),[9] unauthenticated users could directly access and download forms and attachments submitted by member banks, dating back to 2017. The Office of the Chief Information Officer (OCIO) did not initially detect this activity. Some of these attachments were marked as "CONTROLLED," indicating that the content was designated as CUI that is required by FHFA policy to be protected from public release.

Additionally, by altering the CSP website's URL, we could bypass the website's security perimeter and access internal FHFA documents on FHFA's intranet. These documents included risk assessments, policies, internal emails, and CUI-marked files. The CSP website also exposed internal system functions and detailed error messages when incorrect, unexpected, or invalid data was entered. Instead of a generic message such as "Page Not Found," these messages showed additional technical details and code references. We also found three CUI-marked documents posted publicly on the CSP website, in contravention of FHFA's own policies.

Furthermore, using only common tools and various institutional identifers, we were able to masquerade as actual member banks, allowing us to view, edit, and submit Community Support Statements.[10] No strong user authentication controls were required, and the system triggered no alerts of these activities to OCIO's incident response team. FHFA did not enforce basic access controls and did not detect this suspicious, unauthorized activity.

[8] The Federal Home Loan Bank System's collective membership includes roughly 6,500 financial institutions across the country, including large commercial banks, small community banks, credit unions, insurance companies, and community development financial institutions.

[9] A reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A typical URL could have the form http://www.example.com/index.html, which indicates a protocol (http), a host name (www.example.com), and a file name (index.html). Also sometimes referred to as a web address.

[10] The Community Support Statement serves to document a member bank's Community Reinvestment Act performance and support of first-time homebuyers. A member bank subject to CSP review must provide to FHFA: 1) its Community Reinvestment Act rating, if it is subject to the Community Reinvestment Act; and 2) information about its support for first-time homebuyers.

NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* requires that agencies limit system access to authorized users, apply multifactor authentication for stronger identity verification, and ensure all users are uniquely identified. This standard also requires continuous system monitoring to detect suspicious behavior or unauthorized access attempts. For publicly accessible information, controls must prevent unauthorized modifications, adequately protect CUI content, and restrict unauthorized data transmissions. Systems must be securely configured by limiting unnecessary features to reduce potential vulnerabilities and security testing should be conducted during the system development life cycle to identify and remediate flaws. Additionally, protections must be established to suppress internal code or error details from the public. Furthermore, FHFA's internal standards specifically prohibit the public release of CUI unless explicitly authorized and require the removal of any CUI markings from publicly shared content.

FHFA did not sufficiently implement the aforementioned security protections into the CSP website. According to OCIO management, the CSP website was developed by prior OCIO management to replace a fax-based submission process, and then implemented under the direction of the former Office of Housing and Community Investment[11] within the Division of Housing and Mission Goals. The CSP system was developed using various institutional identifiers for authentication, and OCIO did not implement unique logins or multifactor authentication.

Current OCIO officials stated these decisions were made by a prior leadership team and could not explain why member bank submissions or internal documents were accessible without authentication, nor why the CSP website exposed internal system functions and returned detailed error messages.

Regarding the system monitoring, OCIO officials stated that login activity appeared legitimate due to the use of valid member bank credentials, which did not trigger alerts. Based on logs provided, detection occurred only after we triggered error messages while attempting to download files from FHFA's internal network using fuzzing[12] techniques.

OCIO management stated that three documents posted on the CSP website had been incorrectly marked as "CONTROLLED." While the documents have since been reclassified, OCIO officials could not determine the reason for the original mislabeling.

[11] At the end of audit, OCIO informed us that the Office of Housing and Community Investment is no longer in existence. Its functions have been subsumed into the larger Office of Affordable Housing and Community Investment.

[12] Fuzzing or fuzz testing is when invalid data is input into the application through the environment, or input by one process into another process. Fuzz testing is implemented by tools called fuzzers, which are programs or scripts that submit some combination of inputs to the test target to reveal how it responds.

The CSP website's vulnerabilities resulted in a confirmed compromise during audit testing, where non-public internal documents and member bank data were accessed without authentication or detection. Although our testing was a coordinated effort and not a real attack, it demonstrated FHFA's lack of effective controls to prevent unauthorized access, enforce data protections, and monitor for malicious activity. These control deficiencies put the Agency at significant risk of compromise. Had this testing been carried out by a malicious actor, the consequences could have included loss of confidentiality, integrity, and availability of the member bank and FHFA data.

Recommendations

We recommend that the FHFA Chief Information Officer:

1. Develop and implement a plan for strong user authentication controls for all external access to the CSP website in coordination with the new owner of the CSP website, the Office of Affordable Housing and Community Investment.

2. Restrict access to member bank submission forms and associated documents to only authenticated and authorized users.

3. Prevent unauthorized access to internal, CUI, and non-public files through parameter modification in the URL.

4. Remove technical and system level information from public-facing code and pages, including references to internal applications, backend functions, and programming details.

5. Configure all error messages to suppress internal application details and display only user-appropriate messages.

6. Immediately remove all publicly accessible documents containing CUI and review published content for compliance with FHFA's CUI policy.

7. Establish a formal content review and approval process for all documents and content posted to public-facing websites, including checks for CUI data.

8. Deploy monitoring and alerting tools to detect unauthorized logins, document access attempts, or suspicious activity on the CSP website.

9. Segregate public-facing applications from internal networks by re-architecting the CSP website to isolate external access from internal file storage, databases, and infrastructure.

Finding 2: FHFA Approved CSP System for Use Without Complete or Accurate Security Documentation

In 2024, FHFA's Authorizing Official approved the CSP system for continued use without a complete or accurate understanding of its security and privacy posture. This Authority to Operate (ATO)[13] was granted despite significant gaps in the system's control documentation regarding external access. For example, the security Control Assessment[14] did not evaluate how external users, such as member banks, accessed the system in practice. We found that member banks could access the CSP website using various institutional identifiers, a method FHFA never assessed. Furthermore, the System Security and Privacy Plan (SSPP)[15] lacked critical information. The SSPP did not identify that PII is collected by the system, indicate a Privacy Impact Assessment (PIA)[16] was conducted, or clearly explain how the system verifies user identities.

Federal requirements mandate that agencies must fully understand and document how their systems operate before approving them for use. NIST standards and OMB Circular No. A-130, *Managing Information as a Strategic Resource,* require agencies to assess whether security and privacy controls are correctly implemented and functioning as intended. SSPPs must describe these controls, justify any tailoring decisions, and include the results of privacy risk assessments for systems handling PII. FHFA's own standards also require thorough evaluation of risk and formal assessments of how vulnerabilities could affect system security. FHFA's standards also require authorization decisions to be based on complete and risk-informed evidence.

FHFA did not sufficiently meet these requirements. According to OCIO management, the specific cause cannot be conclusively determined due to insufficient historical documentation and institutional knowledge related to the condition. Current OCIO personnel lack direct knowledge of the original decision-making, implementation, and oversight processes that led to this lapse.

[13] Authority to Operate is an official management decision given by a senior federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

[14] A Control Assessment is the testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization.

[15] System Security Privacy Plans provide the security and privacy requirements for the system, along with the controls currently implemented or slated for implementation to meet those requirements.

[16] A Privacy Impact Assessment is an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns.

OCIO management acknowledged this gap and stated that it is taking immediate steps to conduct a retrospective analysis and strengthen documentation, governance, and institutional continuity to prevent recurrence and improve future traceability.

The ATO was authorized without a full understanding of the system's security and privacy posture. Consequently, FHFA leadership lacked complete and accurate information about external access risks and data protection obligations. As demonstrated in our testing of the CSP website as described in Finding 1, this increases the risk of unauthorized access and exfiltration of non-public data, especially when access occurs using only various institutional identifiers or no authentication.

Recommendations

We recommend that the FHFA Chief Information Officer:

10. Ensure that the security control assessor conducts a comprehensive control assessment that evaluates all components, including the CSP website.

11. Reassess the current ATO for the CSP system based on an updated and accurate authorization package and document the resulting authorization decision.

12. Update and approve the SSPP to accurately reflect the system's identification and authentication methods for each user type, describe how the system collects PII, and document that a PIA was completed.

Finding 3: FHFA's Privacy Impact Assessment Did Not Identify Risks Posed by External CSP Users

The CSP system's PIA does not adequately prescribe how external users, such as member banks, access the system or describe the security measures protecting their access. While the PIA describes how member banks submit data through the CSP website, it does not specify the log in process or what security measures protect their access. Specifically, the PIA did not identify that external CSP users rely on various institutional identifiers and are not required to use unique login credentials or multifactor authentication.

Federal privacy and security policies mandate agencies to fully understand and explain how their systems access and protect PII. OMB Circular No. A-130 mandates that agencies have security and privacy controls in place for their information systems, following standards set by NIST. Agencies must also maintain documentation demonstrating how risks are managed and supporting system security decisions, such as performing risk assessments.

Further, OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* mandates that agencies analyze and describe how information will be secured consistent with agency requirements under FISMA. Agencies must confirm compliance with all required federal laws and policies to keep privacy system information secure, demonstrate that they have conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls. Agencies are also required to regularly test their systems to ensure the controls are still working, provide a contact person for user questions, and review system information for potential sensitivity before sharing information from the system publicly.

FHFA did not sufficiently meet these requirements. The PIA did not evaluate how external CSP users accessed the website, nor did it assess the privacy or security risks associated with those access methods. According to OCIO management, the specific cause cannot be conclusively determined due to a lack of sufficient historical documentation and institutional knowledge. Current OCIO personnel do not have direct knowledge of the original decision-making, implementation, or oversight processes that led to this condition. OCIO acknowledged this gap and stated that it is taking immediate steps to conduct a retrospective analysis and strengthen documentation, governance, and institutional continuity to prevent recurrence and improve future traceability.

Because the PIA does not describe how external users access the CSP website, FHFA officials responsible for managing privacy and security are presently unable to fully evaluate the associated risks. This limits FHFA officials' ability to make informed, risk-based decisions regarding authentication, access controls, and data protection for the system. As a result, non-public information submitted by member banks is exposed to increased risk of unauthorized access or disclosure, as demonstrated in our testing.

Recommendation

13. We recommend that the FHFA Chief Information Officer update the PIA to describe how external users access the system, including the security and privacy controls for securing non-public information, in coordination with the Senior Agency Official for Privacy.

Finding 4: FHFA's CCTV Website Was Publicly Accessible and Contained Security Flaws

FHFA's CCTV website was directly accessible from the public internet, despite not being listed in FHFA's inventory of public-facing websites. This website operated over an uncommon communication channel, which made it harder to detect, but no less exposed. The CCTV website allowed access through a login page that did not enforce limits on failed login attempts. We confirmed this by attempting more than 10 invalid logins, none of which triggered any lockout or alert. FHFA's monitoring tools did not detect these activities.

We also found significant vulnerabilities in the CCTV website's construction and maintenance. Its security certificate expired more than five years ago, and its programming code included visible configuration settings, including a default username and password. The site's software had not been updated since at least 2019 and included publicly known security flaws. Furthermore, the website exposed an application programming interface (API),[17] that accepted remote commands over the internet, a feature that, when left unprotected, serves as a major attack surface.

NIST standards require agencies to maintain an accurate inventory of all their systems, ensure those systems are properly maintained, and restrict access to only authorized users. Agencies must regularly update software to fix known vulnerabilities, monitor for suspicious activity, and protect non-public data using encryption and secure configuration. Features like login pages and remote access must include controls such as locking out users after repeated failed attempts and limiting unnecessary functionality. Every system must have a clearly assigned owner responsible for its security throughout its development life cycle.

FHFA did not sufficiently meet these requirements. According to an OCIO official, the CCTV website was implemented approximately 10 years ago and was maintained by two engineers who both retired by 2023. No system owner was designated following their departures, and the website is currently not being maintained. OCIO officials stated that since 2023, other Agency-level priorities had precluded OCIO from backfilling these positions, resulting in a loss of institutional knowledge. As a result, no current OCIO personnel have sufficient familiarity with the historical system design or operation to explain the causes of the identified vulnerabilities, including the public accessibility, uncommon communication channel, and vulnerabilities in access control, authentication, vulnerability management, and secure configuration. The OCIO official was also unaware that the CCTV website was publicly accessible.

The public exposure of FHFA's CCTV website significantly increased the risk to the Agency's physical and information security. Because the site allowed external access, lacked proper authentication controls, contained outdated and vulnerable software, and exposed non-public information in its source code, it could have served as an entry point for malicious activity. These issues increase the risk of unauthorized access to FHFA's security camera feeds, potentially allowing external actors to view, monitor, or manipulate live surveillance footage. This could further cause interruption or compromise of physical security operations, such as facility monitoring or incident response capabilities. Broader cyber intrusion could occur if an attacker were to use the exposed website as a foothold to move deeper into FHFA's internal network.

[17] An API is a system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Additionally, the preventable exposure of a surveillance system that should not have been accessible from the public internet could undermine public trust in the Agency's security practices.

Recommendations

We recommend that the FHFA Chief Information Officer**:**

14. Designate a responsible system owner for the CCTV website to ensure it is actively maintained, in coordination with the appropriate FHFA office.

15. Immediately remove public internet access to the CCTV website or restrict access through network-based controls such as virtual private network or internet protocol allow listing, ensuring it is only accessible by authorized internal users.

16. Update FHFA's public-facing system inventory to include all externally accessible websites and services and establish procedures to validate inventory accuracy on a recurring basis.

17. Apply system hardening measures to the CCTV website by (a) disabling or restricting non-essential ports and services, (b) limiting access to only necessary functionalities, and (c) removing or protecting exposed API from unauthorized use.

18. Enforce authentication and access control by (a) implementing account lockout after a defined number of failed login attempts, (b) enabling logging and alerting for authentication events, and (c) requiring multifactor authentication for administrative or remote access, if supported.

19. Remediate vulnerabilities by (a) applying all available software and firmware updates to the CCTV platform, (b) replacing or renewing expired website security certificates, and (c) conducting a secure code review to identify and remove hardcoded credentials or unsecure configurations.

FHFA COMMENTS AND OIG EVALUATION................................

We provided FHFA management an opportunity to review and provide technical comments on a draft of this audit report. We considered those comments in finalizing this report. In a written response, FHFA management agreed with our recommendations and included the following corrective actions, which we evaluated:

Recommendation 1

> FHFA management responded that it will develop and implement a plan to enhance authentication controls for accessing the CSP website. The response noted that CSP is a biennial program with the current review cycle ending on October 31, 2025, and the next user upload and review cycle will occur in 2027. FHFA plans to implement authentication controls by April 30, 2027, to be available to users for the next participation cycle.
>
> Management's planned corrective actions meet the intent of our recommendation.

Recommendation 2

> FHFA management responded that OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement. The response noted that authentication tokens were added to the bank submissions to restrict unauthorized access, and the capability to retrieve attachments from previous bank submissions was removed.
>
> Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 3

> FHFA management responded that OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement. The response noted that the ability to access files from the application was removed.
>
> Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 4

> FHFA management responded that OCIO completed the corrective actions for this recommendation during the audit engagement. The response noted that OCIO removed the technical and system-level information from system code and pages, including the background functions and programming details.

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 5

FHFA management responded that OCIO completed the corrective action prior to the conclusion of the audit engagement. The response noted that the technical details in the error responses were removed from the CSP website application, and a security update was performed on the system that remediated several of the errors.

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 6

FHFA management responded that OCIO completed the corrective actions for this recommendation during the audit engagement. The response noted that FHFA removed all public-facing CUI from the CSP website. It was also noted that FHFA reviewed and determined the public-facing instructional documents on the CSP website did not contain CUI.

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 7

FHFA management responded that it will ensure that all documents are formally reviewed prior to posting them on public-facing websites, including checks for CUI and sensitive data. The response noted that the review cycle for the current CSP ends on October 31, 2025, and the next user upload and review cycle will occur in 2027. FHFA plans to implement the formal review and approval process for documented contents posted to the public-facing website by April 30, 2027, to coincide with the next review cycle.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 8

FHFA management responded that OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement. The response noted that OCIO had alerting and monitoring tools in place and detected much of the penetration testing activity. It was also noted that alert content was added to notify OCIO of unauthorized log-in access and attempts on the CSP website.

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 9

FHFA management responded that OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement. The response noted that OCIO isolated the CSP website into a secure zone, segregating the public-facing application from the FHFA network.

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 10

FHFA management responded that it will conduct an assessment of all components, including the CSP website, by September 15, 2026.

Management's planned corrective action meets the intent of our recommendation.

Recommendation 11

FHFA management responded that it will conduct a reassessment of the ATO for the CSP system by September 15, 2026.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 12

FHFA management responded that it will update and approve the SSPP to accurately reflect the system's identification and authentication methods for each user type, describe how the system collects PII, and document that a PIA was completed by September 15, 2026.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 13

FHFA management responded that it will update the PIA by September 15, 2026.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 14

FHFA management responded that OCIO had previously completed the corrective action and noted that a designated system owner was in place during the audit engagement. The response also noted that OCIO had previously documented CCTV as a component of the General Support System which had a designated system owner. This was not requested during the audit engagement and therefore was not previously provided to the OIG.

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 15

FHFA management responded that it completed the corrective action prior to the completion of the audit engagement. [Note: Management corrective action, as stated at the exit conference, was to make the CCTV website not publicly accessible.]

Management's corrective action, if implemented as stated, meets the intent of our recommendation.

Recommendation 16

FHFA management responded that during the audit engagement, OCIO removed the public-facing access to the CCTV website. The response also noted that OCIO will establish procedures to validate and update (if needed) the public-facing system inventory accuracy by September 15, 2026.

Management's planned corrective actions meet the intent of our recommendation.

Recommendation 17

FHFA management responded that it completed the corrective actions prior to the conclusion of the audit engagement. [Note: Management corrective actions, as stated at the exit conference, included disabling or restricting non-essential ports and services, limiting access to only necessary functionalities, and removing or protecting exposed API from unauthorized use.]

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 18

FHFA management responded that it completed the corrective actions for this recommendation prior to the conclusion of the audit engagement and noted that the OIG-requested configuration existed and the authentication was in place during the audit engagement. The response also noted that access is granted to specific users through the Agency's Active Directory, which OIG did not have access to at the time of the audit and is subject to and functions under the Agency's security policies. [Note: Management corrective actions, as stated at the exit conference, included enforcing authentication and access control by implementing account lockout after a defined number of failed login attempts, enabling logging and alerting for authentication events, and requiring multifactor authentication for administrative or remote access, if supported.]

Management's corrective actions, if implemented as stated, meet the intent of our recommendation.

Recommendation 19

FHFA management responded that it will remediate the vulnerabilities, including security certificates, hardcoded credentials, and unsecure configurations by September 15, 2026.

Management's planned corrective actions meet the intent of our recommendation.

Overall, we consider FHFA management responsive to the recommendations in this report. These recommendations will remain open until we confirm that corrective actions have been fully implemented. FHFA's written response, in its entirety, is included as Appendix II to this report.

APPENDIX I: METHODOLOGY...

To accomplish our objective, we performed the following procedures:

- Reviewed Government Accountability Office's *Standards for Internal Control in the Federal Government* (GAO-14-704G; September 2014) and determined that the design control activities component was significant to this objective. We focused on the underlying principle that management should: (1) evaluate security threats to information technology from internal and external sources, and (2) design controls over access to protect an entity from inappropriate access and unauthorized use.

- Reviewed the following NIST publications and other federal guidelines:

  - NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (updated December 2020)

  - NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* (September 30, 2008)

  - OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016)

  - OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 26, 2003)

- Signed the Rules of Engagement with FHFA management that outlined the general parameters and period of our testing as well as protocols for reporting any successful intrusions,[18] which is a recommended practice by NIST. In line with the Rules of Engagement, we only attempted to exploit vulnerabilities during agreed upon test windows.

- Conducted external penetration testing of FHFA's network and information systems in four phases: planning, discovery, attack, and reporting:

  - Planning phase: Identified rules, finalized and documented management approval, and set testing goals. This phase sets the groundwork for a successful test. No actual testing occurred in this phase.

[18] An intrusion would have been considered successful if we had gained access to FHFA systems or data, which should have been denied. An intrusion would allow us to view or copy data, monitor user activities, install programs in memory, or otherwise control the target.

  - Discovery phase: During the discovery phase, automated and manual tests were performed to discover FHFA's systems connected to the internet and gather information about those systems. We used various tools and standard operating system functions to find and map network resources. The second part of the discovery phase was a vulnerability assessment that involved manual and automated scanning of the FHFA's public-facing systems to check for known security vulnerabilities. Vulnerabilities that were examined included missing vendor patches, improper configurations, application bugs, default or easy-to-guess passwords, among other things.

  - Attack phase: During the attack phase, we attempted to make use of discovered vulnerabilities to gain unauthorized access to FHFA's network resources. We made use of hardware, software, and manual methods to attempt to exploit FHFA's networks and systems. During this phase, we also conducted a social engineering test of FHFA users. FHFA identified personnel to be excluded from social engineering and included justification for the exclusion. Our tests were conducted outside FHFA's core business hours (9:30 am – 3:30 pm on business days) to the extent practical and consistent with the audit objective and were coordinated with FHFA's point of contact. FHFA provided all the dates and times when the external penetration test could not be performed and provided justifications.

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

- Reviewed the following FHFA policies and procedures to determine FHFA's security controls for their public-facing network and systems:

  - FHFA Access Control Standard, Revision 2.3 (September 30, 2024)

  - FHFA Assessment and Authorization Process, Revision 3.10 (January 13, 2025)

  - FHFA Common Control Plan (November 21, 2024)

  - FHFA Controlled Unclassified Information Policy, Revision 4 (July 8, 2024)

  - FHFA Controlled Unclassified Information Procedures, Revision 2 (March 20, 2023)

  - FHFA Identification and Authentication Standard, Revision 2.2 (September 30, 2024)

    - FHFA Risk Assessment Standard, Revision 2.3 (September 30, 2024)
    - FHFA System Security and Privacy Plan for General Support System (December 4, 2024)
- Interviewed OCIO officials and staff regarding FHFA's implementation of security controls.
- Performed the following vulnerability, penetration, and social engineering tests:
    - Test 1: We connected our OIG test laptops to the internet (external network) to perform network discovery and vulnerability assessment of all FHFA internet-accessible information systems. We used commercial off-the-shelf products, open source, and public domain information security tools to exploit any identified vulnerabilities to gain unauthorized access to FHFA's network and systems. We employed a "black box" testing methodology[19] to assess vulnerabilities and controls, and to evaluate FHFA's network and systems against external threats. We requested that FHFA provide a list of public-facing websites, an inventory of FHFA's external facing systems, and network architecture diagrams. We also requested that FHFA provide internet protocol ranges or subnets to be scanned or excluded from our testing and provide test time limitations. All precautions were taken to avoid any disruption or denial of service to FHFA, other customers, and users of FHFA infrastructure and services, mission functions, and common enterprise services.
    - Test 2: We used our OIG test laptop to setup an external email phishing infrastructure to conduct testing of FHFA's spam protection controls. We attempted to bypass FHFA's email filtering by using our OIG test laptops to send a phishing email that contained suspicious links. We employed a "black box" testing methodology to assess vulnerabilities and controls, and to determine if unauthorized access can be achieved through social engineering. We requested that FHFA provide us with FHFA personnel to be excluded from social engineering and justification for their exclusion.
- We conducted this performance audit between December 2024 and September 2025, at our headquarters in Washington, D.C., in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence

[19] NIST defines black box testing as a test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object.

obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX II: FHFA MANAGEMENT RESPONSE.........................

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

Federal Housing Finance Agency

MEMORANDUM

TO: James Hodges, Deputy Inspector General for Audit

FROM: Luis Campudoni, Chief Information Officer LUIS CAMPUDONI Digitally signed by LUIS CAMPUDONI Date: 2025.09.17 15:51:52 -04'00'

SUBJECT: Management Response for the Draft Report: *Vulnerabilities in FHFA's Public-Facing Systems Risk Unauthorized Access to Non-Public Data.*

DATE: September 17, 2025

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) draft report, which provides the results of OIG's external penetration testing of FHFA's 64 internet-accessible information systems. The objective of OIG's testing was to determine whether FHFA's security controls protect its network and systems against external threats and prevent unauthorized access to FHFA's non-public data.

FHFA agrees with the recommendations in the report, which includes findings for the Community Support Program (CSP) and FHFA's internal video surveillance system (CCTV). Where noted, the Office of the Chief Information Officer (OCIO) has completed corrective actions for the report's recommendations.

As background, the CSP website is used for the submission of Community Support Statements from the Federal Home Loan Banks' member institutions. The CSP does not collect buyer information, loan level data, or safety and soundness information. In addition, the CSP limits external submissions to defined biennial review periods.

Recommendation 1: *Develop and implement a plan for strong user authentication controls for all external access to the CSP website in coordination with the Office of Affordable Housing and Community Investment, which owns the CSP website.*

Management Response: FHFA agrees with the recommendation and will develop and implement a plan to enhance authentication controls for accessing the CSP website. CSP is a biennial program with the current review cycle ending on October 31, 2025. The next user upload and review cycle will occur in 2027. FHFA will implement the authentication controls by April 30, 2027, to be available to users for the next participation cycle.

Recommendation 2: *Restrict access to member bank submission forms and associated documents to only authenticated and authorized users.*

Management Response: FHFA agrees with the recommendation. OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement. Authentication tokens have been added to the bank submissions to restrict unauthorized access. In addition, the capability to retrieve attachments from previous bank submissions has been removed.

Recommendation 3: *Prevent unauthorized access to internal and sensitive files through parameter modification in the URL.*

Management Response: FHFA agrees with the recommendation. OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement. The ability to access files from the application has been removed.

Recommendation 4: *Remove technical and system level information from public-facing code and pages, including references to internal applications, backend functions, and programming details.*

Management Response: FHFA agrees with the recommendation. OCIO completed the corrective actions for this recommendation during the audit engagement. OCIO has removed the technical and system-level information from system code and pages, including the background functions and programming details.

Recommendation 5: *Configure all error messages to suppress internal application details and display only user-appropriate messages.*

Management Response: FHFA agrees with the recommendation. OCIO completed the corrective action prior to the conclusion of the audit engagement. The technical details in the error responses have been removed from the CSP website application, and a security update was performed on the system that has remediated several of the errors.

Recommendation 6: *Immediately remove all publicly accessible documents containing CUI and review published content for compliance with FHFA's CUI policy.*

Management Response FHFA agrees with the recommendation, and OCIO completed the corrective actions for this recommendation during the audit engagement. FHFA removed all public facing Controlled Unclassified Information (CUI) from the CSP website. FHFA reviewed and determined the public-facing instructional documents on the CSP website did not contain CUI.

Recommendation 7: *Establish a formal content review and approval process for all documents and content posted to public-facing websites, including checks for CUI and sensitive data.*

Management Response: FHFA agrees with the recommendation. FHFA will ensure that all documents are formally reviewed prior to posting them on public-facing websites, including checks for CUI and sensitive data. The review cycle for the current CSP ends on October 31, 2025. The next user upload and review cycle will occur in 2027, as CSP is a biennial program. FHFA will implement the formal review and approval process for documented contents posted to the public-facing website by April 30, 2027, to coincide with the next review cycle.

Recommendation 8: *Deploy monitoring and alerting tools to detect unauthorized logins, document access attempts, or suspicious activity on the CSP website.*

Management Response: FHFA agrees with the recommendation. OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement. OCIO had alerting and monitoring tools in place and detected much of the penetration testing activity. Additionally, alert content was added to notify OCIO of unauthorized log-in access and attempts on the CSP website.

Recommendation 9: *Segregate public-facing applications from internal networks by re-architecting the CSP website to isolate external access from internal file storage, databases, and infrastructure.*

Management Response: FHFA agrees with the recommendation. OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement. OCIO has isolated the CSP website into a secure zone, segregating the public-facing application from the FHFA network.

Recommendation 10*: Ensure that the security control assessor conducts a comprehensive control assessment that evaluates all components, including the CSP website.*

Management Response: FHFA agrees with the recommendation and will conduct an assessment of all components, including the CSP website, by September 15, 2026.

Recommendation 11: *Reassess the current ATO for the CSP system based on an updated and accurate authorization package and document the resulting authorization decision.*

Management Response: FHFA agrees with the recommendation and will conduct a reassessment of the Authority to Operate (ATO) for the CSP system by September 15, 2026.

Recommendation 12: *Update and approve the SSPP to accurately reflect the system's identification and authentication methods for each user type, describe how the system collects PII, and document that a PIA was completed.*

Management Response: FHFA agrees with the recommendation and will update and approve the System Security and Privacy Plan (SSPP) to accurately reflect the system's identification and authentication methods for each user type, describe how the system collects PII, and document that a PIA was completed by September 15, 2026.

Recommendation 13: *We recommend that the FHFA Chief Information Officer update the PIA to describe how external users access the system, including the security and privacy controls for securing sensitive information, in coordination with the Senior Agency Official for Privacy.*

Management Response: FHFA agrees with the recommendation and will update the PIA by September 15, 2026.

Recommendation 14: *Designate a responsible system owner for the CCTV website to ensure it is actively maintained, in coordination with the appropriate FHFA office.*

Management Response: FHFA agrees with the recommendation. OCIO had previously completed the corrective action, and notes that a designated system owner was in place during the audit engagement. OCIO had previously documented CCTV as a component of the GSS system which had a designated system owner. This was not requested during the audit engagement and therefore was not previously provided to the OIG.

Recommendation 15: *Immediately remove public internet access to the CCTV website or restrict access through network-based controls such as a virtual private network or internet protocol allow listing, ensuring it is only accessible by authorized internal users.*

Management Response: FHFA agrees with the recommendation and completed the corrective action prior to the completion of the audit engagement.

Recommendation 16: *Update FHFA's public-facing system inventory to include all externally accessible websites and services and establish procedures to validate inventory accuracy on a recurring basis.*

Management Response: FHFA agrees with this recommendation. During the audit engagement, OCIO removed the public-facing access to the CCTV website. OCIO will establish procedures to validate and update (if needed) the public-facing system inventory accuracy by September 15, 2026.

Recommendation 17: *Apply system hardening measures to the CCTV website by (a) disabling or restricting non-essential ports and services, (b) limiting access to only necessary functionalities, and (c) removing or protecting exposed API from unauthorized use.*

Management Response: FHFA agrees with the recommendation. OCIO completed the corrective actions prior to the conclusion of the audit engagement.

Recommendation 18*:* *Enforce authentication and access control by (a) implementing account lockout after a defined number of failed login attempts, (b) enabling logging and alerting for authentication events, and (c) requiring multifactor authentication for administrative or remote access, if supported.*

Management Response: FHFA agrees with the recommendation. OCIO completed the corrective actions for this recommendation prior to the conclusion of the audit engagement, and notes that the OIG requested configuration existed and the authentication was in place during the audit engagement. Access is granted to specific users through the Agency's Active Directory, which OIG did not have access at the time of the audit and is subject to and functions under the Agency's security policies.

Recommendation 19: *Remediate vulnerabilities by (a) applying all available software and firmware updates to the CCTV platform, (b) replacing or renewing expired website security certificates, and (c) conducting a secure code review to identify and remove hardcoded credentials or unsecure configurations.*

Management Response: FHFA agrees with the recommendation and will remediate the vulnerabilities, including security certificates, hardcoded credentials**,** and unsecure configurations by September 15, 2026.

cc: Marcus Williams
Edom Aweke
John Major
Warren Hammonds
Jeffery Harris

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