OFFICE of INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Interim Report: FHA Catalyst Personally Identifiable Information Risk Management in a Zero Trust Environment

Washington, DC | 2023-OE-0007a

October 31, 2024

Office of Evaluation | Office of Inspector General
U.S. Department of Housing and Urban Development

Date: October 31, 2024

To: Jeffrey Little
General Deputy Assistant Secretary of Housing, H

Sairah Ijaz
Acting Chief Information Officer, Q

From: John Garceau
Acting Assistant Inspector General for Evaluation, G

Subject: Interim Report: FHA Catalyst – Personally Identifiable Information Risk Management in a Zero Trust Environment

Please find attached an interim evaluation on the Office of Housing's progress toward implementing the requirements of the Zero Trust Architecture data and identity pillars for FHA Catalyst. The purpose of this evaluation is to inform you of observations we made while conducting Office of the Inspector General (OIG) evaluation 2023-OE-0007, HUD's Personally Identifiable Information Risk Management in a Zero Trust Environment. The FHA Catalyst system was selected as a sample system for that evaluation.

We provide three recommendations and four opportunities for improvement specific to Housing and FHA Catalyst, with only the recommendations being formally tracked by our office.

The Inspector General Act, 5 U.S.C. § 420, requires that OIG post its reports on the OIG website. Accordingly, this report will be posted at https://www.hudoig.gov.

Please do not hesitate to contact me with any questions or concerns at (202) 603-8410 or jgarceau@hudoig.gov.

Attachment

cc:
Juan Sargent, Acting Principal Deputy Chief Information Officer, Q
Trent Nickles, Acting Chief Administrative Officer, Office of Administration A1
Paul Scott, Business Change and Integration Officer – CIO, Q
Ahmed Jamal Bouaichi, Senior Advisor, Business Change and Integration Office – CIO, Q
Porter Davis, Audit Liaison Officer, QMAC

The following record is a HUD OIG document; however, all redactions applied within it were asserted by HUD, which operates under a separate regulatory authority apart from HUD OIG, to protect the interests of that agency and its stakeholders.

This page intentionally left blank

Executive Summary

INTERIM REPORT FHA CATALYST PERSONALLY IDENTIFIABLE INFORMATION RISK MANAGEMENT IN A ZERO TRUST ENVIRONMENT | 2023-OE-0007A

Purpose

We evaluated the U.S. Department of Housing and Urban Development (HUD) Office of Housing's (Housing) progress in applying zero trust security principles to protect personally identifiable information (PII) within the Federal Housing Administration (FHA) Catalyst system.

Executive Order (EO) 14028 required agencies to move towards zero trust architecture (ZTA) to protect critical data and modernize cybersecurity. Office of Management and Budget (OMB) Memorandum M-22-09 set forth a Federal zero trust strategy and associated milestones. The Cybersecurity Infrastructure Security Agency (CISA) developed a maturity model to assist agencies in measuring their zero trust progress in five areas or pillars (identity, devices, networks, applications and workloads, and data).

Our objective was to assess the effectiveness of Housing's zero trust initiatives for the data and identity pillars and use the CISA maturity model to measure Housing's maturity in those two areas with focus on FHA Catalyst.

Findings

Repeated system ownership transitions and leadership changes continued to cause project management challenges for FHA Catalyst and the ability to implement zero trust.

HUD lacked automation capabilities and visibility into its data. Lack of visibility increases the risk of data breach, as HUD is unable to monitor its data movement.

Housing began to implement phishing-resistant multifactor authentication (MFA) on FHA Catalyst in FY 2024 but did not meet EO 14028 and M-22-09 milestones. Fully implementing phishing-resistant MFA will reduce the risk of identity compromise and strengthen the security of FHA Catalyst.

Housing lacked dynamic access controls, consistent reviews of logs and accounts, and automation capabilities. Without the ability to automate account management, there is an increased risk of an insider threat or a user with unnecessary access to personally identifiable information.

Recommendations

In this report we offer three new recommendations and four opportunities for improvement (OFI) to Housing. These OFIs will not be tracked as formal recommendations but are noted as general suggestions for Housing to improve its zero trust architecture implementation.

Table of Contents

Introduction

BACKGROUND

Through a zero trust cybersecurity approach, an organization does not trust any user, device, or network by default. It requires continuous verification of identity and permissions for accessing resources. Executive Order (EO) 14028, Improving the Nation's Cybersecurity, stresses the critical need for a zero trust architecture to protect critical data, such as personally identifiable information (PII). The Cybersecurity and Infrastructure Security Agency (CISA) notes that the path to zero trust is an incremental process that may take years to implement.

The Office of Management and Budget (OMB) issued Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, which sets forth a Federal zero trust architecture strategy requiring agencies to meet specific cybersecurity standards and objectives by the end of fiscal year (FY) 2024 to reinforce the Government's defenses. In response to M-22-09, HUD developed a Zero Trust Strategy Implementation Plan in April 2022, in which HUD identified actions it would take to implement zero trust. However, in FY 2024, HUD had shifted its zero trust priorities yet had not updated its implementation plan and was establishing its project management for zero trust. HUD had made little progress in establishing the enterprise guidance and solutions necessary for program offices to implement zero trust.

In support of EO 14028 and M-22-09, CISA issued a maturity model to measure agency progress in five zero trust pillars, as shown in figures 1 and 2 below.

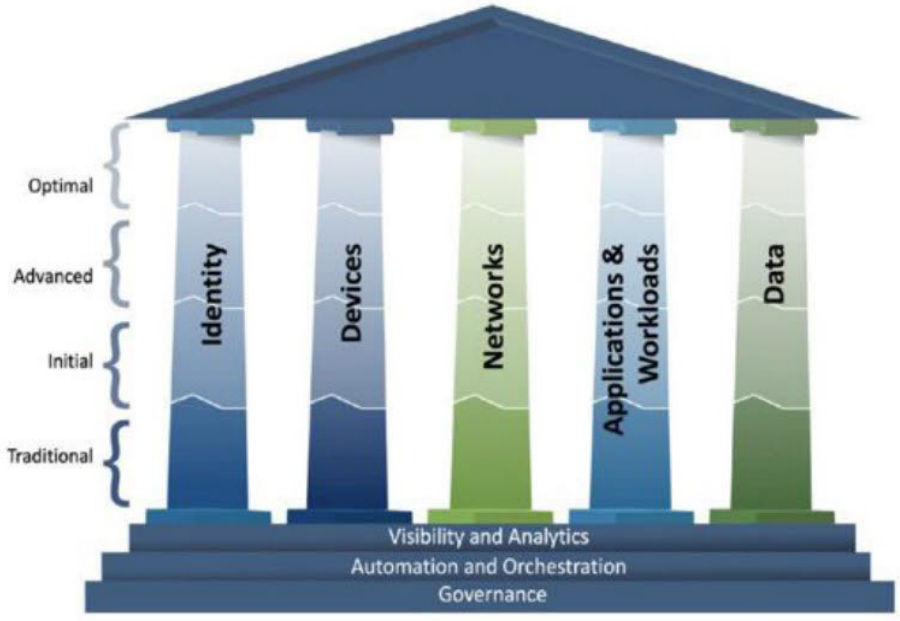

Figure 1: CISA Zero Trust Maturity Evolution

CISA's Zero Trust Maturity model ranges from a traditional maturity level, in which there is no implementation of zero trust controls to optimal maturity that fully implements zero trust, this progress is represented in figure 2 below. At the traditional level, security controls are manually configured, and security policies are static. At the initial level, the agency starts automation of controls and policies, starts integrating external systems with its zero trust controls, and is in the beginning stages of visibility into systems. At the advanced level, the agency implements automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination. In addition, the agency establishes centralized visibility, and is building toward enterprise-wide awareness. At the optimal level, the agency has fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated observed triggers, cross-pillar interoperability with continuous monitoring, and centralized visibility with comprehensive situational awareness.

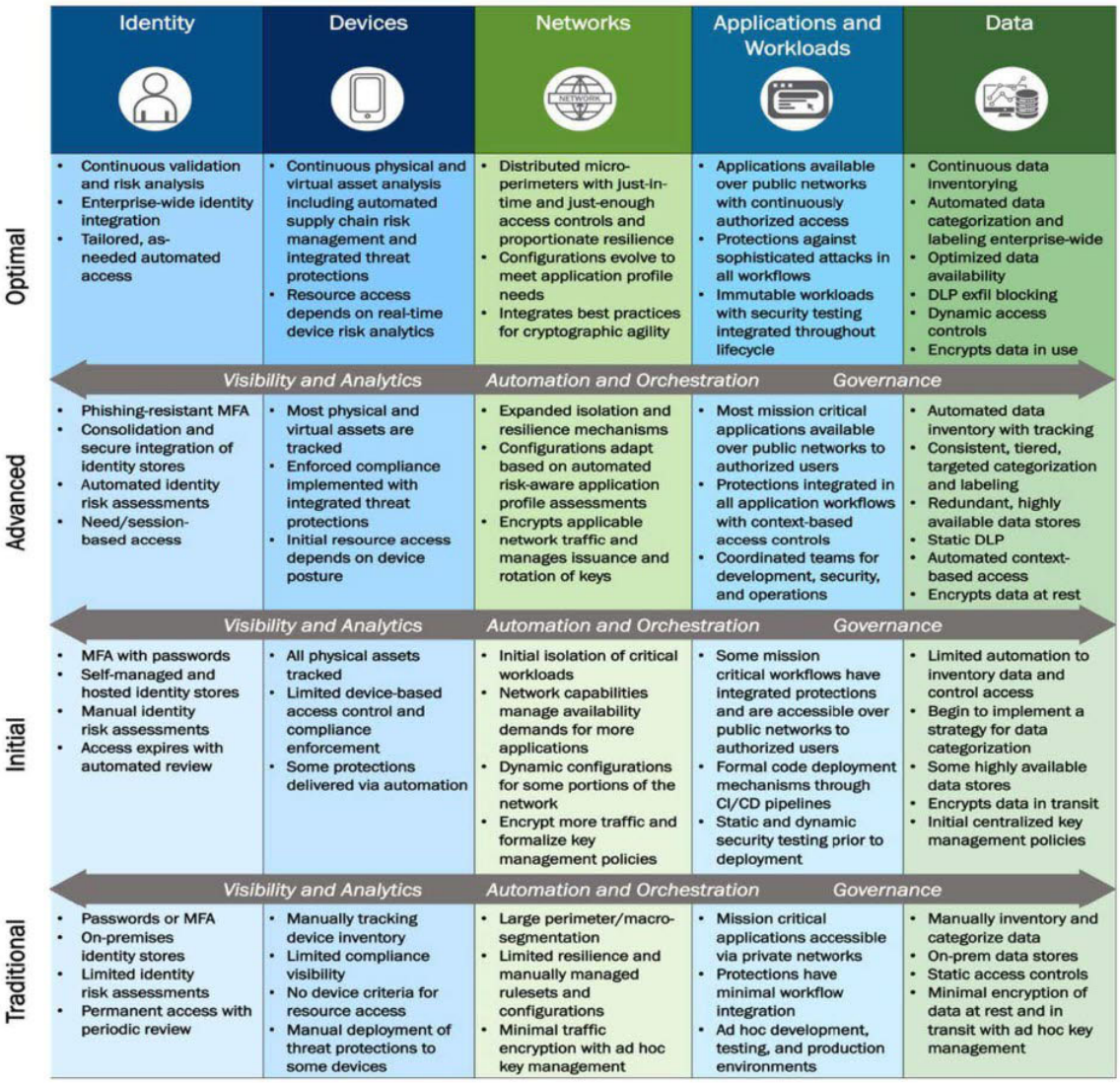

Figure 2: CISA High-Level Zero Trust Maturity Model Overview

We selected FHA Catalyst as a sample system to review as part of our evaluation 2023-OE-0007, HUD's Personally Identifiable Information (PII) Risk Management in a Zero Trust Environment. We assessed the progress made by the Office of Housing toward implementing identity and data zero trust controls for FHA Catalyst. Our scope for this interim report was limited to the FHA Catalyst system and any U.S. Department of Housing and Urban Development (HUD) policies, processes, or technical support required by FHA Catalyst as part of its operating environment. We considered key enterprise-, program-, and system-level evidence in effect as of May 2024.

We conducted this evaluation in accordance with the Quality Standards for Inspection and Evaluation (December 2020), issued by the Council of the Inspectors General on Integrity and Efficiency.[1] Those standards require that we plan and perform the evaluation in a manner that allows us to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions.

Results of Review

SUMMARY

HUD is in the beginning stages of implementing zero trust requirements for the data and identity pillars. HUD's Housing systems, including FHA Catalyst, are largely dependent on enterprise initiatives and technical solutions to effectively implement many zero trust controls. Therefore, we rated zero trust implementation for FHA Catalyst at the lower maturity levels for the data and identity pillars. We made the following key observations:

Data pillar: CISA ZTA maturity model describes the data pillar as, "agency data should be protected on devices, in applications, and on networks in accordance with federal requirements. Agencies should inventory, categorize, and label data; protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration. Agencies should carefully craft and review data governance policies to ensure all data lifecycle security aspects are appropriately enforced across the enterprise."

Housing conducts data inventories but is unable to automate the process and has not yet included FHA Catalyst in its inventories. Housing is also unable to (b)(5) because HUD lacked enterprise data management processes, standards, and technical solutions. As a result, Housing cannot (b)(5) (b)(5) in its systems, including FHA Catalyst.

Identity pillar: CISA ZTA maturity model describes the identity pillar as, "agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access. Agencies should integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities. Agencies should integrate their identity stores and management systems, where appropriate, to enhance awareness of enterprise identities and their associated responsibilities and authorities."

[1] Quality Standards for Inspection and Evaluation (ignet.gov)

HUD prioritized the rollout of phishing-resistant multifactor authentication (MFA) and is nearing full implementation for FHA Catalyst. However, Housing has not applied dynamic access controls within FHA Catalyst to (b)(5) (b)(5) FHA Catalyst further lacks the capability for automated user activity logging, which is necessary to detect anomalies and help identify potential attacks. Housing also does not review user accounts with sufficient frequency to help reduce access risks, including insider threats.

FINDINGS

Challenges in FHA Catalyst Project Management

FHA Catalyst is an essential modernization for HUD and its mortgage industry partners' execution of FHA mortgage insurance programs. The system is intended to streamline processes of the program and protect it against cybersecurity threats.[2] FHA Catalyst originated as a Housing system in December 2020, with ownership transferring to the Office of the Chief Information Officer (OCIO) after initial development in 2021. System ownership transitioned back to Housing in August 2023. These transitions contributed to delays in system development, including the exhaustion of funds and decisions by HUD's Executive Steering Committee that impacted the prioritization of FHA Catalyst.[3] This system is an integral part of Housing's March 2024 strategic roadmap that aligns with HUD's enterprise IT modernization roadmap. However, this strategic roadmap did not address zero trust requirements.

FHA Catalyst provides benefits to both HUD users and lenders, which ensure that it is a competitive product in the marketplace. The user-friendly interface supports a modernized work environment for HUD employees using the system. Additionally, lenders report that FHA Catalyst effectively supports their business needs. Housing recently issued a survey to lenders, which reported that FHA Catalyst has enabled a

- 21 percent reduction in lender data entry errors
- 42 percent reduction in staff time
- 47 percent reduction in staff time managing case binder.

While FHA Catalyst has provided business process improvements for system users, it also faces challenges that pose a risk for HUD. First, FHA Catalyst interacts with multiple HUD legacy systems, which can cause issues when the legacy systems are unable to implement zero trust functions. Legacy systems also inherently contain more security vulnerabilities,[4] exposing FHA Catalyst to additional risk. FHA Catalyst will continue to be impacted by legacy systems if HUD does not consistently move away from these systems across the agency.

Second, Housing has established some practices and procedures in support of zero trust; however, it is highly dependent on enterprise initiatives to implement the tools and the infrastructure required to meet zero trust requirements. For example, (b)(5) (b)(5) (b)(5) HUD, at the enterprise level, is responsible for developing zero trust technical controls

[2] See HUD IT Modernization Roadmap Evaluation Report for additional information.
[3] See Delays in Federal Housing Administration Catalyst's Development (hudoig.gov) for additional information.
[4] HUD IT Modernization Roadmap Evaluation Report

through enterprise architecture. Until HUD further develops a zero trust implementation roadmap, program offices cannot fully implement technical controls that help protect sensitive information, including PII. HUD's zero trust implementation will require effective project management with a robust roadmap that addresses all five zero trust pillars and an implementation plan to ensure that technical solutions are integrated with the HUD enterprise architecture and efficiently rolled out to programs and applications.

Since FY 2019 FHA Catalyst has relied on earmarked development, modernization, and enhancement (DME) funding. However, no earmarked DME funding for FHA Catalyst was including in the president's budget in FY 2025 although DME funding is needed for continued development. HUD received $8 million in zero trust initiatives for FY 2025, which will support implementation of MFA, and FHA Catalyst will be directly impacted by receiving MFA through this funding. Additionally, Housing leadership reported a reduction in funding due to inflation. Maintenance costs for essentials continue to increase; therefore, operations and maintenance are requiring more funding. DME funding supports the modernization necessary to secure sensitive information.

FHA Catalyst Had Not Implemented Critical Zero Trust Data Functions

CISA's data pillar is divided into eight functions, which help guide agencies to protect all data within its environment. The eight functions include data inventory and management, data categorization, data availability, data access, data encryption, visibility and analytics, automation and orchestration, and governance. All functions have controls that ensure data is properly secured in all stages of the data lifecycle.

Housing was reliant on the Chief Data Officer and OCIO to develop enterprise solutions required to address many data function requirements. However, HUD had made little progress in developing standards and procedures or implementing technical solutions to support program office zero trust data initiatives. For example, (b)(5)
(b)(5)
(b)(5) We found an overall lack of automation, centralization, and defined strategies and processes required to implement robust data management technology and support other zero trust pillars.

The average FHA Catalyst score for data functions represents a maturity between the traditional and initial levels described in figure 2. The score is bolstered by an advanced rating for the data availability function. FHA Catalyst is hosted by AWS GovCloud, an approved government cloud solution that provides highly available data storage and multiple failover (backup) locations and strong encryption for data. We noted that most data functions were dependent on enterprise policy, procedures, or technical solutions. See table 1 below.

Table 1: FHA Catalyst data pillar ratings

Function	1 - Traditional	2 - Initial	3 - Advanced	4 - Optimal
Data inventory and management	(b)(5)			
Data categorization				
Data availability				
Data access				
Data encryption				
Visibility and analytics				
Automation and orchestration				
Governance				

Housing does not have an automated data inventory capability and documented its PII data through manual processes. In accordance with agency procedures, Housing conducted thorough privacy impact assessments (PIA) to identify the PII in each system and completed a PIA for the FHA Catalyst system. Housing went beyond agency requirements by also developing and maintaining an extensive manual records-data inventory. Housing uses that inventory to (b)(5) (b)(5) Further, the Housing records management liaison officer maintains a (b)(5) (b)(5) None of these manual processes provide an automated capability to (b)(5) (b)(5) For these capabilities, Housing is dependent on the Chief Data Officer and OCIO to complete HUD's enterprise strategy and implement a technical data resource management solution to automate its data inventory. Both of these enterprise initiatives were underway.

To protect its data, an agency must know specifically what data it has and where the data are located within the broader HUD environment. Failure to comprehensively identify and inventory its data prevents Housing from fully understanding data locations, types, and uses, including its most critical data. Without this information, it cannot implement appropriate data exfiltration controls, which depend on knowing where data are, who is authorized to access the data, and where the data can and cannot be transferred. Lack of insight also impedes the ability to determine whether systems such as FHA Catalyst maintain only PII that is relevant and necessary to achieve the agency mission.

There is no data categorization or labeling in place for FHA Catalyst. Housing describes the types of PII maintained within its systems through the PIA process and generally tracks the types of data in its systems through its manual data inventory. HUD had also applied broad categorizations of data, such as (b)(5) and the Chief Data Officer is working towards a data management solution to help with enterprise data categorization. However, without standard

enterprise data categorizations and labels, Housing lacks the schema[5] needed to protect data in a tiered, targeted manner and apply specific controls to protect each specific type of data. Without a process to digitally tag sensitive data, it could not apply more stringent technical access controls to those data. This issue created the risk that Housing's more sensitive data were not protected with more assurance than its less sensitive data.

Access controls are primarily manual and provide no capability to incorporate key risk attributes. HUD's Digital Identity Access Management System (DIAMS) provides a level of automated access for user account provisioning, and Housing generally applies the principle of least privilege when granting access to FHA Catalyst. However, the system's technical access controls were limited and did not incorporate key attributes such as (b)(5) (b)(5) Failure to incorporate these attributes limited the effectiveness of FHA Catalyst access controls

Housing has limited data visibility and capability to track sensitive data including FHA Catalyst data. HUD implemented several new technologies within the past two years to improve general data visibility across its network and systems. However, without automated processes to identify, inventory, label, and tag data, HUD's ability to track and monitor specific data is restricted, and the benefit from this technology is limited. User activity logging for FHA Catalyst is also not robust, and Housing has limited ability to detect anomalies in data access, use, or movement. This limited visibility restricts Housing's ability to recognize ongoing risk to its sensitive data.

FHA Catalyst Began to Implement Zero Trust Identity Functions

CISA's identity pillar is divided into seven functions, which help agencies establish controls to ensure users only have access at the right time and right purpose with no excessive access. The seven functions include authentication, identity stores, risk assessments, access management, visibility and analytics, automation and orchestration, and governance.

The average FHA Catalyst score for identity functions represents an (b)(5) though it achieved an (b)(5) for authentication and governance. HUD prioritized the identity functions, enabling Housing to implement certain identity controls for FHA Catalyst, such as phishing-resistant MFA. Housing is reliant on OCIO to develop a roadmap and implement the technical solutions that will be required to address many required identity functions. However, identity functions within the purview of Housing and the FHA Catalyst system are not implemented. These include developing more (b)(5) (b)(5) (b)(5) Additionally, some automation capabilities required for identity functions need collaboration between OCIO and Housing for full implementation. See table 2 below.

[5] The organizational structure used to store data.

Table 2: FHA Catalyst identity pillar ratings

Function	1 - Traditional	2 - Initial	3 - Advanced	4 - Optimal
Authentication	(b)(5)			
Identity stores[6]				
Identity risk assessments				
Access management				
Visibility and analytics				
Automation and orchestration				
Governance				

HUD has begun implementing phishing-resistant MFA to strengthen the authentication process for FHA Catalyst. Phishing-resistant MFA is one of the most secure ways of authenticating users and provides a significant level of protection at the application level. In FY 2024, HUD completed deployment of its MFA solution to internal FHA Catalyst users and plans to complete deployment for external users by the end of FY 2025.

FHA Catalyst does not limit access based on user actions and resource needs. Housing consistently assesses user access needs based on their user role and need to know before granting initial access to FHA Catalyst. However, implementing access controls that are dynamic, are tailored to user actions, and require continuous reauthentication would reduce the risk of an insider threat. Examples include attribute-based access controls that are logically constructed around a specific application's functionality and tailored to the individual user's role and the need for access to complete an authorized process in the proper sequence at an appropriate time of day. Reducing continuous access to unnecessary information reduces the impact of an attack from a potential insider threat. (b)(5) (b)(5) however, granular access controls have not been implemented.

HUD lacks an automated identity risk assessment process. HUD consistently implemented identity risk assessments; however, the process is not automated and does not include a quality control review procedure. This manual process can introduce subjectivity and inconsistency. Implementing automation for identity risk will help bring consistency to the process. Automation removes the human factor, which may include subjective ratings with assurance levels associated with a system. Additionally, the more user risks the system can identify, the more prepared the system team can be in preventing an attack associated with identity. HUD has implemented a user behavior analysis tool to help assign risks to users based on their activity on a system. However, this tool has not yet been implemented within FHA Catalyst.

[6] The identity stores function calls for consolidation and integration of identity stores across agency applications. The maturity level for this function is assessed at the enterprise level versus the system level.

Housing has limited log automation and inconsistent log reviews. HUD defined and logged audit events necessary to monitor business transactions of interest for FHA Catalyst. These logs are generated yearly or when requested by system administrators. The ISSO plans to (b)(5) (b)(5) Housing is reliant on HUD's Security Operations Center (SOC) for cybersecurity event logging; however, HUD's SOC had not met OMB's M-21-31 logging capabilities[7].

M-21-31 established a four-tier maturity model (not effective, basic, intermediate, and advanced) to categorize agency logging capabilities and required agencies to be at advanced logging capabilities by August 2023. In April 2024, HUD was working to achieve basic logging capabilities for all systems, including FHA Catalyst. Logging increases visibility of user actions and helps system administrators ensure that user activity within a system is normal. Without increased logging capabilities and reviews of user activity logs, it is difficult to identify discrepancies or potential attacks.

Housing lacks automation and consistency for user account reviews. Housing implemented limited automation for account management through DIAMS, including automated emails to system security administrators for account creation, deletion, or change in access. However, Housing's review of FHA Catalyst user accounts is a manual process and completed annually as part of HUD's authorization to operate (ATO)[8] requirements. The annual review of accounts does not comply with HUD Access Control Supplement Guide, which requires quarterly account reviews. Consistent provisioning of user identities is important to ensure that users who need access to the system have it and users who do not need access to the system do not. Inconsistent, manual review of accounts allows for the possibility of a user having incorrect access and leaves the system vulnerable to an insider threat in which a user may have unintended, unauthorized access to an FHA Catalyst module. Insider threats are dangerous because there are many opportunities for data loss, including the potential that the threat actor could release information that was not made for public consumption. Consistent reviews with automation that check for discrepancies could help mitigate this risk.

FHA Catalyst is not enrolled in HUD's ongoing authorization process. FHA Catalyst's only confirmation of implementation of technical controls that protect PII is through the ATO process, in which all controls are reviewed over a 3 year cycle. In April 2024, Housing was (b)(5) (b)(5) (b)(5) Without continuous enforcement of identity controls, it is possible for a control to be improperly implemented and the error to go unnoticed until the system's next ATO cycle. This issue could leave the system at risk for a variety of attacks surrounding access and accounts and reduce overall security.

[7] M-21-31 established requirements to improve visibility "before, during, and after a cybersecurity incident" by requiring agencies to record such events to improve incident detection and response.
[8] An ATO is a formal declaration issued by a senior official that determines the risk of operating an information system and authorizes the system to operate in a particular security environment.

Conclusion

Housing is in the beginning stages of implementing zero trust data and identity controls for its systems, including FHA Catalyst. At the enterprise level, HUD has prioritized the implementation of key identity controls for all systems, resulting in a slightly higher maturity level for the identity pillar for FHA Catalyst.

While Housing and FHA Catalyst are significantly dependent on enterprise solutions and initiatives to address many of the zero trust data and identity requirements, there are actions that Housing can potentially take in support of zero trust initiatives.

RECOMMENDATIONS

1. Housing should include zero trust requirements as part of the Housing Strategic Roadmap for Housing Modernization.

2. Housing should refine access controls within the FHA Catalyst modules that are dynamic, are tailored to user actions, and require continuous reauthentication to ensure that users have access only to information needed.

3. Housing should coordinate with HUD's SOC to
    a. Ensure that FHA Catalyst user behavior monitoring logs are regularly captured and adequately reviewed for discrepancies in user activities.
    b. Establish program office responsibility for the log review process.

OPPORTUNITIES FOR IMPROVEMENT

1. Housing should collaborate with the Chief Data Officer in assessing opportunities to support enterprise data categorization initiatives, particularly as part of any modernization efforts involving FHA Catalyst or other Housing systems.

2. Housing should collaborate with Housing Records Management Liaison Officer (RMLO) to ensure the inclusion of FHA Catalyst PII data and other system information in the overall Housing records/data inventory process on a quarterly basis.

3. Housing should determine whether FHA Catalyst's Cloud platform technology would enable additional logging and alerting of access or data movement anomalies.

4. In accordance with HUD's Access Control Supplement Guide, Housing should complete quarterly account reviews for all users within FHA Catalyst. These reviews should determine if users have the correct access and there are no unnecessary users within the system.

Appendix A – Agency Comments and OIG's Response

AGENCY COMMENTS

Docusign Envelope ID: 66D01B7A-9710-4BDD-9CD5-F4E1422E1948

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

WASHINGTON, D.C. 20410-3000

September 26, 2024

MEMORANDUM FOR: John Garceau
Acting Assistant Inspector General for Evaluation, G

DocuSigned by:
Jeffrey Little
3515450E447042D...
9/27/2024

FROM: Jeffrey Little
General Deputy Assistant Secretary of Housing, H

DocuSigned by:
Sairah R. Ijaz
F230FDB9B68248D...
9/27/2024

Sairah Ijaz
Acting Chief Information Officer, Q

SUBJECT: Draft Interim Report: FHA Catalyst – Personally Identifiable Information Risk Management in a Zero Trust Environment

Thank you for the opportunity to review and respond to the draft report on Personally Identifiable Information Risk Management in a Zero Trust Environment (2023-OE-0007). The Office of Housing and the Office of the Chief Information Officer share in your commitment to managing data proactively in a Zero Trust Environment.

To date, the Department has taken notable steps toward our shared goal. We highlight just a few of those steps here:

1) Housing appointed an Information System Security Officer (ISSO), Privacy Liaison Officer (PLO), and Senior Advisor for IT Modernization to support FHA Catalyst, building on the Authorization to Operate (ATO) successfully completed in September 2024. Many of the issues raised during the evaluation were addressed during the ATO process.
2) Housing established System Security Administrators and backups for each module within FHA Catalyst to ensure access is role-based and continuously monitored.
3) OCIO has procured Salesforce Shield and Salesforce Data Mask which will allow for automated monitoring of data events and preventative data encryption and obfuscation.

Housing and OCIO will continue working together to address specific items in Report 2023-OE-0007. Specifically, FHA Catalyst and Zero Trust team leads have partnered to implement Enhanced Identity Credential and Access Management (EICAM) effort not only in FHA Catalyst but enterprise-wide, thus ensuring compliance with M-22-09 requirements.

cc:
Juan Sargent, Acting Principal Deputy Chief Information Officer, Q
Trent Nickles, Acting Chief Administrative Officer, Office of Administration A1
Paul Scott, Business Change and Integration Officer – CIO, Q
Porter Davis, Audit Liaison Officer, QMAC

OIG RESPONSE

We requested that Housing and OCIO provide formal comments in response to our draft report indicating agreement or disagreement with our recommendations. Housing and OCIO provided a joint response and did not concur or non-concur with any recommendations in the report. HUD stated that these comments were in response to the HUD PII Risk Management in a Zero Trust Environment (2023-OE-0007); however, this report specifically addresses Housing's management of PII within FHA Catalyst (2023-OE-0007a).

The status of recommendations 1, 2, and 3 will remain "unresolved-open" until we receive and agree to HUD's proposed management decisions for each recommendation. We will contact both Housing and OCIO shortly after the issuance of this report to discuss the recommendations.

In its formal comments, Housing and OCIO said they have taken notable steps to managing data proactively in a zero trust environment. Some of these steps include appointing an Information System Security Officer (ISSO), Privacy Liaison Officer (PLO), and Senior Advisor for IT Modernization, establishing System Security Administrators and backups for each module, and procuring tools to enhance automated monitoring of data events and enhance preventative data encryption and obfuscation. We note these steps taken and encourage the continued implementation of zero trust architecture capabilities.

HUD also stated the issues raised during the evaluation were addressed through the completion of the authorization to operate (ATO) for FHA Catalyst in September 2024. HUD's ATO process requires the Office of Information Technology Security (OITS) and Privacy Office assessors to conduct security and privacy assessments on a subset of controls and provide assessment results on an annual basis. The Authorizing Official (AO) uses the annual assessment results to make Ongoing Authorization (OA) decisions annually, which informs a system's ATO approval every three years.

Although FHA Catalyst recently completed its ATO in September 2024, HUD also concurred that OCIO and Housing will continue working together to address the specific findings and associated recommendations and opportunities for improvement from this report. For example, during its ATO exercise, HUD created a plan of action and milestone (POA&M) to address user activity logging as required by OMB M-21-31. This relates to one of our recommendations within this report. Our other recommendations address project management and dynamic user access controls, which were not addressed during the ATO process.

We appreciate the assistance that HUD staff provided throughout the evaluation and Housing and OCIO's commitment to address the report results. We look forward to working with Housing and OCIO to reach a management decision on the unresolved, open recommendations in this report.

Appendix B – List of Abbreviations

Acronym	Definition
AO	authorizing official
ATO	authority to operate
CISA	Cybersecurity and Infrastructure Security Agency
DIAMS	Digital Identity Access Management System
DME	development, modernization, and enhancement
EO	executive order
FHA	Federal Housing Authority
FY	fiscal year
Housing	U.S. Department of Housing and Urban Development Office of Housing
HUD	U.S. Department of Housing and Urban Development
ISSO	Information System Security Officer
M	memorandum
MFA	multifactor authentication
OA	ongoing authorization
OCIO	Office of the Chief Information Officer
OFI	opportunity for improvement
OIG	Office of Inspector General
ROMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
PLO	Privacy Liaison Officer
POA&M	plan of action and milestone
ZTA	zero-trust architecture

Appendix C – Acknowledgements

This report was prepared under the direction of John Garceau, Acting Assistant Inspector General for Evaluation, and Kirk Van Camp, Acting Director of the Information Technology Evaluations Division. The Office of Evaluation staff members who contributed are recognized below.

MAJOR CONTRIBUTORS

Kenzie Averill, Senior IT Evaluator
Craig Wood, Senior IT Evaluator