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

The U.S. Department of Housing and Urban Development's Personally Identifiable Information Risk Management in a Zero Trust Environment

Washington, DC | 2023-OE-0007

December 12, 2024

Information Technology Evaluations Division | Office of Inspector General
U.S. Department of Housing and Urban Development

Date: December 12, 2024

To: Sairah Ijaz
Chief Information Officer, Q

Trent Nickels
Acting Chief Administrative Officer, A1

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

Subject: Final Report – U.S. Department of Housing and Urban Development's Personally Identifiable Information Risk Management in a Zero Trust Environment

Attached is the U.S. Department of Housing and Urban Development (HUD), Office of Inspector General's (OIG) final report on HUD's personally identifiable information (PII) risk management in a zero trust environment evaluation.

In this evaluation, we found that HUD maintains a significant number of records that contain PII, HUD did not develop and maintain a detailed implementation plan or timeline for zero trust initiatives, and HUD had significant organizational and technical challenges to overcome to implement a zero trust architecture.

We provide six new recommendations and three opportunities for improvement, 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. This report is a controlled document and should be released only to those within the Department or to employees of an information technology contractor with a need to know this information.

Enclosures:

Final HUD's Personally Identifiable Information Risk Management in a Zero Trust Environment (2023-OE-0007)

Cc:

Juan Sargeant, Acting Deputy Chief Information Officer
Christina Addison, Acting Chief Information Security Officer
Vinay Singh, Chief Financial Officer
Jeffrey Little, General Deputy Assistant Secretary for Housing

Todd Richardson, Acting Chief Data Officer
Damon Smith, General Counsel
Gayle Bohling, Deputy General Counsel for Operations
Paul Scott, Assistant Chief Information Officer, Planning, Policy, and Performance
Porter Davis, Office of the Chief Information Officer Audit Liaison Officer

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

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT'S PERSONALLY IDENTIFIABLE INFORMATION RISK MANAGEMENT IN A ZERO TRUST ENVIRONMENT | 2023-OE-0007

Purpose

In a zero trust cybersecurity model, no user, system, network, or service operating outside or within an organization's security perimeter is trusted. This strategy places significant emphasis on stronger enterprise identity and access controls.[1] Organizations must continually authenticate each user, device, application, and transaction rather than rely on one initial authentication at the network or application level. A zero trust approach significantly reduces risk by explicitly verifying users; categorizing and strictly limiting access to data resources, eliminating open-ended access permissions; and providing situational awareness into each instance of data access.

Executive Order (EO) 14028 required agencies to move toward zero trust architecture (ZTA) to protect critical data and modernize cybersecurity. Office of Management and Budget Memorandum M-22-09 set forth a Federal zero trust strategy and milestones, and 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).

We evaluated the U.S. Department of Housing and Urban Development's (HUD) progress in applying zero trust security principles to protect its personally identifiable information (PII).

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

Findings

HUD had not determined the volume of PII it manages.

HUD did not have an automated process to inventory or categorize data, which restricted its visibility into its PII. We issued surveys to HUD program offices to estimate the magnitude of PII maintained by HUD and found that HUD systems hold an estimated 16.3 billion records that contain PII. This figure far exceeds the approximate 1 billion PII records that HUD offices last reported to us in 2018.[2]

HUD had not updated its ZTA implementation plan.

HUD developed an initial zero trust implementation plan in FY 2022, which identified data as the most critical ZTA element and identified the development of a supporting data platform architecture as its top ZTA priority. By FY 2024, HUD had not achieved this goal and was focusing on identity pillar initiatives but had not updated this plan to reflect any changes in its zero trust priorities or activities.

---

[1] OMB M-22-09

[2] OIG conducted similar surveys of PII record counts as part of privacy evaluations conducted in 2014 and 2018 (2014-ITED-0001 and 2018-OE-0001).

HUD Lacked Resources to Implement ZTA.

HUD had assigned project managers and key roles to oversee zero trust initiatives but continued to face potential resourcing and organizational challenges, including HUD had not estimated the actual number of personnel needed for zero trust initiatives.

HUD Did Not Consistently Identify Risks Associated with ZTA.

HUD monitored information technology (IT) and cybersecurity risks through its OCIO risk register process. However, the register did not contain specific ZTA implementation risks. It identified only one data risk on this register and did not consider other risks associated with lack of zero trust implementation.

HUD Did Not Ensure That Systems Implemented Dynamic Access Controls.

HUD did not ensure that systems applied granular access controls, including just-in-time and just-enough access tailored to individual actions and individual resource needs. Doing so would reduce the risks posed by providing permanent or standing access to PII and sensitive information.

HUD Was Delayed in Implementing Phishing-Resistant Multifactor Authentication.

Agencies were required to implement multifactor authentication (MFA) by November 2021 and phishing-resistant MFA to external users by January 2023. As of May 2024, HUD had begun phishing-resistant MFA implementation of one of its authentication systems for internal users.

Recommendations

In this report, we offer six new recommendations and three opportunities for improvement (OFI). These OFIs will not be tracked as formal recommendations but are noted as general suggestions for HUD. The recommendations should help HUD improve its ZTA planning and move forward in key ZTA areas including data inventory and categorization, access control, and risk management.

Table of Contents

Introduction

BACKGROUND

Executive Order (EO) 14028,[3] issued in May 2021, emphasized the need for agencies to move toward a zero trust architecture (ZTA) to protect critical data and modernize cybersecurity. In a zero trust model, no user, system, network, or service operating outside or within the security perimeter is trusted. Agencies must continually authenticate each user, device, application, and transaction rather than relying on one initial authentication at the perimeter of a network or initial access to an application. This strategy places significant emphasis on stronger enterprise identity and access controls.[4]

In January 2022, the Office of Management and Budget (OMB) issued Memorandum M-22-09, which laid out a ZTA strategy and required agencies to meet specific cybersecurity standards and objectives by the end of fiscal year (FY) 2024. These standards were aligned with the Cybersecurity Infrastructure Security Agency (CISA) ZTA maturity model,[5] which was developed to assist agencies in measuring their zero trust progress and maturity. This model identified five areas or "pillars" (identity, devices, networks, applications and workloads, and data) that encapsulate zero trust concepts. For this evaluation, we focused on how the U.S. Department of Housing and Urban Development (HUD) implemented the data and identity pillars' functions to protect personally identifiable information (PII). For more details, see appendixes B and C.

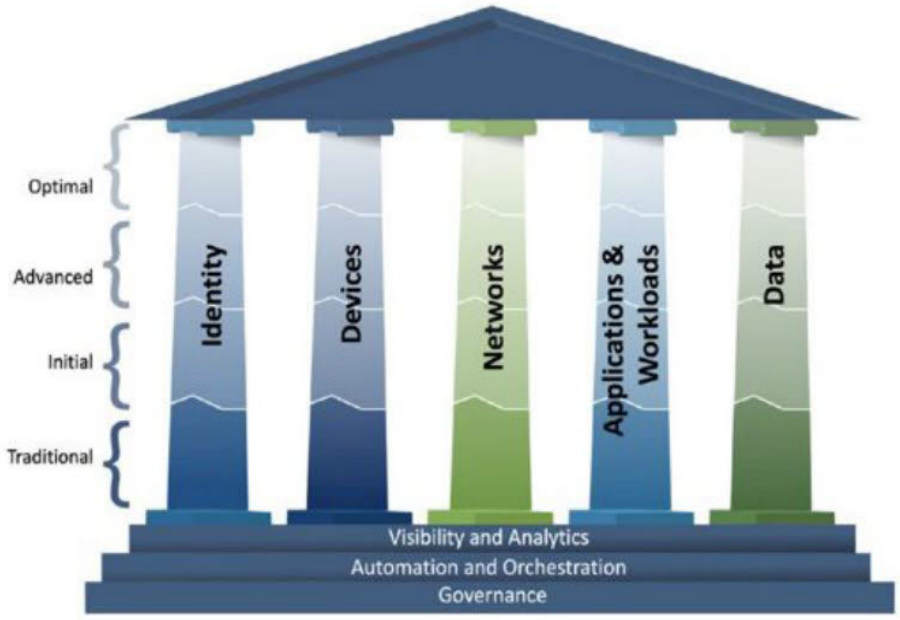

Figure 1. CISA zero trust maturity evolution

[3] EO 14028
[4] OMB M-22-09
[5] CISA Zero Trust Maturity Model

HUD maintains significant amounts of PII[6] within many of its systems due to the nature of the services it provides. Various HUD systems maintain multiple types of PII records, such as Social Security number, date of birth, banking information, and other financial information. HUD is responsible for protecting stakeholder PII data from data breach; therefore, implementing controls to protect and restrict access to these data must be an agency priority.

In the past two years, HUD significantly matured its privacy program and its overall governance of PII. The Privacy Office updated its policies and procedures, integrated its system authorization processes with the Office of the Chief Information Officer (OCIO), designated privacy liaison officers across the agency, enhanced the specialized training provided to personnel with significant privacy responsibilities, instituted a compliance program, and developed dashboards to monitor operational performance. Further, the Chief Privacy Officer conducted a gap analysis to identify program inefficiencies and identify legal requirements that HUD did not address. HUD directed additional resources to the privacy program to address those deficiencies. As of December 2024, HUD had addressed and closed 60 of 67 recommendations provided in our past privacy evaluations.

The foundational improvements to HUD's privacy program focused on key managerial and operational controls. However, HUD had limited technical controls required to protect PII and build an effective ZTA to better manage risk in today's threat environment. Critically, as noted in the CISA maturity model, agencies must establish automated processes and systems to move toward optimal zero trust maturity. Implementation of zero trust is critical to protect PII, as the technical controls enable greater security and control over sensitive data.

In July 2024, OMB issued M-24-14, which requires agencies to submit an updated zero trust implementation plan to OMB and the Office of the National Cyber Director by November 7, 2024. This plan will provide HUD an opportunity to develop its desired future state for zero trust, identify its current capabilities and gaps to address, and determine the requisite resources and timeline to address the gaps to achieve its desired future state. HUD had assigned project managers to oversee zero trust initiatives and support the plan HUD establishes.

OBJECTIVE

Our objective was to evaluate HUD's ability to identify and protect its PII and access to PII using zero trust principles. We used CISA's ZTA maturity model to assess the agency's implementation of all data and identity functions, including technical implementation of these controls on two HUD systems, (b)(5) (b)(5) (b)(5) Appendix B describes the scope and methodology used to conduct the evaluation.

[6] The National Institute of Standards and Technology (NIST) Computer Security Resource Center defines PII as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Results of Review

SUMMARY

HUD maintained a significant number of records that contain PII with limited zero trust controls in place to secure these data. In FY 2022, HUD established a zero trust implementation plan to help the agency address the five zero trust pillars established by CISA; however, by FY 2024, HUD had made limited progress in the initiatives established in its plan. In FY 2024, HUD began to implement some technical controls to support identity pillar functions but lacked overall direction and a clear plan to make significant zero trust progress.

PII INVENTORY IN THE HUD ENVIRONMENT

HUD is entrusted with protecting the PII of tens of millions of Americans. We found that HUD had not completed a central inventory to determine the volume of PII maintained in its environment, which restricted its understanding of the potential risk and impact presented by its information systems.

HUD had processes to identify its mission critical data and high-value assets and to inventory and determine the general security category of each system. HUD assessed the data in each system to identify, describe, and list each information type, including PII, and to determine the PII confidentiality impact level (PCIL) for each system. HUD had also started to use automation tools to identify PII located on its network outside its official information systems, such as on user laptops.

However, HUD did not have standards and processes in place for conducting data inventories or categorizing and labeling data as required within the ZTA data pillar. The Office of the Inspector General (OIG) has consistently reported in prior evaluations[7] that HUD had not developed an automated process to fully identify, inventory, categorize, and label its information, which prevented it from fully understanding the locations, types, uses, and movement of sensitive data such as PII. This lack of data insight impacts the effectiveness of multiple security controls. For example, data exfiltration controls depend on knowing where data are, who is authorized to access data, and where data can and cannot be transferred. Without a complete data inventory, HUD was also unable to ensure that it maintained only PII that was relevant and necessary for meeting the agency's business purposes and mission.

The absence of an automated categorization and labeling process impacted HUD's ability to prioritize the protection of its most critical information in a tiered, targeted manner. For example, without labeling and applying persistent tags to track its most sensitive data, HUD could not ensure that it consistently applied more stringent access controls to those data or identify which specific data may merit continuous monitoring for unusual activity protection. This deficiency created the risk that HUD's most sensitive data may be protected with no more assurance than its least sensitive data.

We issued surveys, conducted interviews with program offices, and assessed documentation to estimate the magnitude of PII maintained by HUD systems. The privacy liaison officers (PLO) within HUD program offices self-reported that more than 70 percent of HUD systems contain PII, with an estimated total of

[7] HUD Office of Evaluation Reports 2014-ITED-0001, 2018-OE-0001, and 2019-OE-0002a.

16.3 billion[8] records holding some type of PII. The PII record counts provided by the PLOs are listed in Table 1 below. OCIO reported five systems contained PII, but did not report PII record counts for these systems. Because HUD does not have an automated process to fully identify and inventory its PII, this count may be underestimated. HUD relies on privacy impact assessments and PII PCIL determinations to document which systems contain PII, but these procedures do not require program offices to maintain an automated and continuous count of records containing PII. A compromise of even a portion of this sensitive information through a data breach could result in significant financial loss to both HUD and the people HUD services and a damaged reputation for being unable to protect the personal information of its stakeholders.

Table 1: PII record count as of May 2024

Program office	Number of records that contain PII
Office of Policy Development and Research	13,000,000,000
Office of Housing	2,423,168,960
Office of the Chief Financial Officer	676,261,565
Office of Community Planning and Development	200,000,000
Office of Fair Housing and Equal Opportunity	26,000,000
Office of Public and Indian Housing	16,061,016
Office of the Chief Human Capital Officer	16,000
Office of the Chief Administrative Officer	8,151
Office of the General Counsel	6,000
Government National Mortgage Association[9]	42,500,000
Office of the Chief Information Officer[10]	did not report
Office of Lead Hazard Control and Healthy Homes	0
Total	**16,384,021,692**

As noted in EO 14028 and OMB M-22-09, agencies can no longer depend on conventional defenses to protect critical systems and data, and slow and inconsistent deployment of newer cybersecurity tools and practices leaves an organization exposed to adversaries. Transitioning to a zero trust approach provides a defensible architecture for the new threat environment. Further, the implementation of a vision, in which security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information should help HUD secure its vast amount of PII.

HUD'S ZERO TRUST PLAN

[8] (b)(5)

[9] GNMA reported PII records as part of the scope of this evaluation; however, HUD's zero trust strategic plan does not encapsulate GNMA or its systems.

[10] OCIO reported five systems contained PII, but did not report PII record counts for these systems.

We reviewed HUD's plan from FY 2022 and actions to move toward implementing zero trust and found that HUD did not develop and maintain a detailed implementation plan or timeline for zero trust initiatives.

Historical Zero Trust Plan

On April 4, 2022, HUD released its zero trust implementation plan as required by OMB M-22-09. This plan established how HUD planned to address zero trust requirements. HUD identified the data pillar functions as the highest priority for the agency to address. The plan also addressed functions of the identity pillar.

For the data pillar, HUD's first objective was to design and implement a platform architecture that would enable it to accurately discover and categorize datasets, govern data access, and identify malicious use of sensitive data. This objective would support zero trust, simplify HUD's enterprise architecture, and allow HUD to produce consistent policies. However, HUD provided no further information and did not provide a response to M-22-09's requirements for a strategy to identify milestones and a technical approach for categorizing and tagging data.

For the identity pillar, HUD identified tools and processes it was implementing to support zero trust functions and determined identity function plans for future implementation. In FY 2022, HUD made limited progress towards implementing identity controls, such as the implementation of some access management and governance controls at a low maturity level. HUD stated that to improve its identity functions, it would need to implement an enterprise-wide identity, credential, and access management (ICAM) solution to help with authentication, account management, and overall governance. However, in its Zero Trust Strategy Implementation Plan, HUD stated that obtaining the necessary budgetary resources would present a challenge to implementing a centralized identity management system. HUD submitted a Technology Modernization Fund request in May 2021 for $28.3 million for cybersecurity support for ICAM initiatives; however, HUD was awarded $14.8 million.

FY 2024 Zero Trust Plan

In FY 2024, HUD was prioritizing its zero trust identity pillar initiatives but had not updated its ZTA implementation plan to reflect this change in priorities. HUD did not have detailed implementation plans that included milestones for the zero trust data and identity pillars. OCIO was the overall lead for HUD's ZTA implementation, with the Enterprise Architect (EA) being the lead for the identity pillar, and the Chief Data Officer (CDO) being the lead for the data pillar.

OCIO's and the EA's priority zero trust initiative in FY 2024 was to start implementing phishing-resistant multifactor authentication (MFA). HUD began implementing phishing-resistant MFA through one of its authentication systems beginning with internal users in FY 2024. The completion of phishing-resistant MFA on all systems will require coordination between OCIO and program offices. OCIO will provide the tool for the authentication capability to the systems, and the program offices must then integrate that capability into their systems. EO 14028 required agencies to implement MFA by November 2021, and M-22-09 required agencies to implement phishing-resistant MFA to external users by January 2023. However, HUD had not met EO 14028 and M-22-09 requirements by May 2024.

HUD's highest priority data initiative was to develop an initial master data inventory and an automated inventory capability to support ZTA. In FY 2024, HUD identified a data model and tool for this purpose and projected that it would require two to three years to fully develop the tool into an integrated data resource management solution. The CDO was developing a performance work statement and obtaining contractor assistance for this inventory initiative.

The CDO was working with the Chief Technology Officer and the EA on data definitions and models for HUD's enterprise architecture. The CDO was also coordinating with the privacy office, the records office, and program offices as they developed new systems to identify opportunities for creating metadata to support data governance and ZTA. Data labeling will be the responsibility of the CDO in coordination with program offices. Once completed, the labeling will provide the source for open data requirements and reporting to Congress, in addition to supporting ZTA.

In July 2024, OMB issued M-24-14, which required agencies to submit an updated zero trust implementation plan to OMB and the Office of the National Cyber Director by November 7, 2024. The memorandum also states that agencies must self-rate and document current and target maturity levels in each pillar for all high-value assets and high-impact systems.[11] An updated, accurate plan would help HUD prioritize initiatives and identify areas of improvement to reach a zero trust environment.

ZERO TRUST CHALLENGES

HUD faced Significant Organizational and Resourcing Challenges for Implementing ZTA

HUD assigned key roles and responsibilities for leading HUD's zero trust initiatives but continued to face potential resourcing and organizational challenges and had not identified the number of personnel required to implement ZTA. HUD had experienced delays in hiring for several key positions[12], including two hiring actions that had been ongoing for nearly a year. OCIO was designated as the ZTA lead and had identified the need to create a project charter and designate leads for each ZTA pillar. However, OCIO was still working to determine the best structure for managing the project and noted the concern with HUD's history of failing to successfully sustain and fully implement projects.

OCIO had designated leads for the data and identity pillars and expressed the critical need for future integration among all pillars for zero trust and having a defined future state for ZTA. This will be especially important for the data pillar, as its lead, the CDO, is not in OCIO but will be integral to successful ZTA implementation. For the data pillar, HUD established an overall data governance charter and board, which it anticipated would help support ZTA data pillar initiatives. However, HUD had not developed a data pillar implementation plan and had not determined the number of personnel that would be needed to implement data pillar requirements. For the identity pillar, HUD was assessing gaps and planned to create a more refined implementation plan.

HUD Identified Limited Risks Associated with Zero Trust

HUD identified detailed information technology (IT) and cybersecurity risks through its OCIO risk register process. However, the register did not contain specific ZTA implementation risks that would enable HUD to prioritize the numerous initiatives required to implement ZTA, or to identify potential threats associated with failure to implement specific ZTA functions. The register contained one generic risk that failure to implement adequate safeguards aligning with ZTA principles could expose confidential information and result in reputational harm to the agency. At the enterprise risk management level, zero trust was not specifically mentioned in conjunction with any risk area.

[11] HUD OIG did not assess HUD's progress on this requirement, as the scope of this evaluation ended in May 2024. In November 2024, HUD stated it completed a new implementation plan and submitted to OMB as required.
[12] HUD officials reported that these delays were primarily due to HUD's lengthy hiring process.

HUD Had Inconsistent Access Controls

Access management is critical for both the data and identity pillars to reach higher levels of maturity for zero trust. Advanced levels require agencies to assign attributes and implement need-based and session-based controls. Optimal levels require agencies to implement just-in-time and just-enough access tailored to individual actions and individual resource needs. HUD access controls were managed by the program offices, and while HUD had guidance through its IT Security Control Catalog, many program offices did not implement the granular controls on their systems required for advanced or optimal maturity.

(b)(5)

(b)(5)

Implementing access controls to ensure that users have access only to information needed to do their immediate task protects against an insider threat and a potential data breach. Data and identity zero trust access functions require agencies to implement attribute-based controls to reduce this risk. HUD's legacy systems may present a challenge for implementation of dynamic access controls due to outdated custom code or unsupported or end-of-life technology. To better protect the PII of people HUD serves, HUD must improve controls to access systems and PII.

HUD Faced Challenges with Deploying MFA

Phishing-resistant MFA on all systems is required for agencies to reach advanced and optimal maturity levels of the authentication function for zero trust. HUD began to implement phishing-resistant MFA authentication to internal users in FY 2024, although it did not meet EO 14028 and M-22-09 requirements. HUD planned to implement phishing-resistant MFA on all systems, but there are challenges HUD will face. First, HUD had multiple authentication systems in use; therefore, to implement phishing-resistant MFA on all systems, HUD will have to coordinate individual integration with each of these authentication systems. Second, there could be issues with requiring some users to authenticate with phishing-resistant MFA, and HUD had not established a solution for these nontraditional users. Lastly, HUD established a plan to fully implement phishing-resistant MFA with milestones, but the plan did not include dates associated with reaching these milestones. In the modern threat landscape, usernames and passwords are not a secure form of authentication. Any password can be guessed with the right tools and time. Phishing-resistant MFA is a solution to traditional username and password methods that helps to prevent password attacks and a threat gaining access to HUD systems.

Conclusion

HUD's Privacy Office had success in the last few years establishing managerial and operational controls to improve its overall privacy governance; however, HUD made less progress in implementing technical controls to support zero trust architecture. In FY 2024, HUD had not developed a detailed implementation plan or timeline for zero trust initiatives, faced significant organizational and resourcing challenges to implementing ZTA, identified limited risks associated with zero trust, lacked an automated data inventory and categorization capability, did not ensure that dynamic access controls were implemented across the agency, and faced challenges with phishing-resistant MFA implementation. While HUD had made limited progress toward implementing ZTA, an updated plan with specific milestones addressing technical implementation should support HUD in addressing its challenges.

Recommendations

1. HUD OCIO should identify needs to address Federal requirements by performing a gap analysis on its zero trust architecture strategic plan.

2. HUD OCIO should establish a zero trust architecture implementation plan that includes milestones and resources to address all zero trust pillars.

3. The CDO should coordinate with HUD's Records Office, Privacy Office, and program offices to develop data policies and procedures for data inventory, categorization, and labeling in support of zero trust architecture.

4. HUD OCIO should develop system policies and procedures for dynamic access controls that include just-in-time and just-enough access tailored to individual actions and individual resource needs.

5. HUD's Privacy Office should require program offices to periodically review systems in all environments (testing, development, production) for unnecessary disclosure of personally identifiable information (PII).

6. HUD OCIO should capture risks that are associated with zero trust architecture implementation and document these risks in its risk register.

Opportunities for Improvement

1. HUD officials responsible for each zero trust pillar should coordinate and collaborate on initiatives throughout the implementation of zero trust architecture.

2. HUD Chief Data Officer (CDO) should develop a ZTA data implementation plan.

3. OCIO and the CDO should strategize on how to apply persistent data tags once categorization and labeling are complete.

Appendixes

APPENDIX A – AGENCY COMMENTS AND OIG'S RESPONSE

Agency Comments

Docusign Envelope ID: A9393C2C-DDD9-46DB-A864-2497FF812B70

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, D.C. 20410-3000

CHIEF INFORMATION OFFICER

November 22, 2024

MEMORANDUM FOR: John Garceau
Acting Assistant Inspector General for Evaluation, Office of Inspector General (HUD OIG)

FROM: Paul Scott PAS
Assistant Chief Information Officer, Planning, Policy, and Performance (ITPPP) Office of Chief Information Officer (CIO)

SUBJECT: HUD comments to Draft PII Risk Management in a Zero Trust Environment (2023-OE-0007)

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). We share commitment to proactively protect and manage data in a zero trust environment.

The Department has made substantial progress in implementing zero trust architecture and protecting PII in recent years. Key achievements include:

- In November 2023, deployed phishing-resistant MFA to 9 FHA-Connection systems serving external users.
- In November 2023, HUD completed a discovery of zero trust capabilities and gaps through a third-party assessment. This assessment informed the development of our enterprise implementation strategy aligned with NIST 800-207, OMB M-22-09, and CISA's zero trust maturity model.
- In June 2024, HUD CIO published a memorandum titled "Advancing Zero Trust Architecture: Enterprise-wide Implementation of Phishing-Resistant MFA," detailing successful deployment to pilot systems and outlining the strategy for department-wide expansion.
- Conducted ongoing enterprise architecture reviews with technical experts to design comprehensive ICAM solutions, refining implementation roadmap based on evolving requirements and capabilities.
- As of September 2024, expanded secure authentication across HUD's enterprise by implementing phishing-resistant MFA on 28 systems and standard MFA on 33 additional systems, strengthening our identity security posture.
- In September 2024, secured a $19.8 million Technology Modernization Fund award based on successful implementation of phishing-resistant MFA pilot. This funding enables enterprise-wide expansion of ICAM capabilities.
- Awarded strategic ICAM contracts in FY2024 for professional services, legacy system modernization analysis, and program management to support enterprise-wide implementation, including policy development and strategic planning.

Docusign Envelope ID: A9393C2C-DDD9-46DB-A864-2497FF812B70

- In November 2024, submitted an updated Zero Trust Implementation Plan to OMB that aligns with OMB M-24-14 requirements, detailing HUD's enterprise strategy and implementation milestones through FY2025.
- Developing comprehensive ICAM policy, targeted for FY2025 release, that establishes specific identity security requirements aligned with M-22-09 and NIST 800-207 that strengthens enterprise-wide access management controls.

While the report highlights certain concerns, it does not fully reflect these significant improvements or our ongoing initiatives. OCIO will continue implementing risk-based solutions to address remaining gaps identified in the report. We appreciate the opportunity to review and provide comments on this report. We look forward to continuing collaboration with OIG to strengthen HUD's cybersecurity posture.

Summary of the U.S. Department of Housing and Urban Development (HUD) Comments and the Office of Inspector General Response

We requested that HUD provide formal comments in response to our draft report indicating agreement or disagreement with our recommendations. HUD did not concur or non-concur with any recommendations in the report.

The status of recommendations in this report will remain "unresolved-open" until we receive and agree to HUD's proposed management decision for each recommendation.

In its formal comments, HUD reported additional actions it has taken since May 2024 to further implement zero trust architecture which was after the conclusion of this evaluation's fieldwork. HUD stated it had outlined a strategy and implemented phishing-resistant MFA to additional systems, and had secured a $19.8 million Technology Modernization Fund award that will enable enterprise-wide expansion of ICAM capabilities. HUD reported it conducted ongoing enterprise architecture reviews and analyzing legacy system modernization in support of future ICAM solutions. We acknowledge these steps taken and encourage these types of initiatives that will continue to improve HUD's zero trust architecture and protection of personally identifiable information.

HUD stated that phishing-resistant MFA was implemented on nine systems through FHA Connection as of November 2023. However, the evidence collected during this evaluation, including documentation and interviews with HUD personnel, indicated that phishing-resistant MFA was at the beginning stages of implementation. The phishing-resistant MFA Deployment Approach and the Strategic Plan were provided as evidence, yet neither identified specific implementation dates. This report reflects this status of implementation and notes that phishing-resistant MFA was implemented on one authentication system at the time of the evaluation but does not identify the number of HUD systems that received phishing-resistant MFA through this authentication system. HUD stated as part of the FY24 Q2 FISMA reporting, 62 systems utilized MFA. However, not all these 62 systems utilize phishing-resistant MFA as required by the CISA Zero Trust Maturity Model.

HUD also stated that in November 2023, it conducted a discovery of zero trust capabilities and gaps through a third-party assessment. HUD did not provide this assessment as evidence of its zero trust initiatives, although, during interviews HUD officials stated the need to conduct such a zero trust gap analysis. HUD did provide its Zero Trust Strategic Implementation Plan from 2022 which is stated in this report.

Additionally, HUD provided technical comments to this report which the OIG reviewed and made requested minor changes to the report.

We appreciate the assistance that HUD staff provided throughout the evaluation. We look forward to working with HUD to reach a management decision on the unresolved, open recommendations in this report.

APPENDIX B – SCOPE, METHODOLOGY, AND LIMITATIONS

Scope

The scope of our review was departmentwide and included HUD policies, procedures, and practices relating to the identity and data pillars of the U.S. Department of Homeland Security's (DHS) CISA ZTA maturity model. Our review covered the period January through May 2024. Our scope included all HUD programs and systems. Additionally, we selected two sample systems to assess technical implementation of zero trust controls.

Methodology

We conducted this evaluation in accordance with the Quality Standards for Inspections and Evaluation (December 2020) issued by the Council of the Inspectors General on Integrity and Efficiency.[13] 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.

We used OMB, National Institute of Standards and Technology (NIST), and DHS guidance to determine requirements for the DHS CISA ZTA maturity model and assessed the level of agency progress in addressing the identity and data pillar functions outlined by the CISA model. Our approach included the following techniques:

- Inquiries with management and systems personnel.
- Issuance of a survey to agency privacy liaison officers (PLO) and analysis of responses.
- Inspection of documentation related to the implementation of zero trust requirements.
- Inspection of reports (for example, recent OIG evaluation reports) related to this evaluation.
- Data calls to program offices and system points of contact to gather accurate program data.
- Queries of HUD's Cybersecurity Assessment and Management (CSAM) system to obtain system artifacts.
- Virtual interviews and demonstrations to gain an understanding of data and identity programs and practices and system operations.
- Referenced select security controls from NIST Special Publication 800-53, Revision 5, that relate to the DHS CISA ZTA maturity model.
- Security testing to verify the implementation of technical controls.[14]

We evaluated the following organization levels to accomplish our objectives:

Department level – During this step, we gained an understanding of the zero trust policies and guidance that HUD OCIO and the Office of the Chief Data Officer established for HUD. We compared HUD's policies, procedures, and practices to applicable zero trust guidance and criteria to determine overall agency progress in meeting Federal ZTA requirements.

---

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

[14] Identity and data controls were also assessed as part of the FY 2024 FISMA Evaluation (2024-OE-0002) and FY 2024 FISMA Penetration Test Evaluation (2024-OE-0002a).

Program office and system level – We gained an understanding of and assessed the implementation of zero trust policies and procedures across HUD. Our objective was to obtain this understanding in terms of "program perspective." We conducted virtual interviews with program office personnel, including all privacy liaison officers, to review all survey responses and discuss zero trust implementation within each program office. We further assessed the implementation of zero trust policies and procedures for two specific systems, (b)(5) (see table 2 below), and conducted a full assessment of zero trust maturity for the FHA Catalyst system. The results of the FHA Catalyst zero trust maturity assessment were provided in a separate report.[15]

Table 2: Systems assessed using the CISA ZTA maturity model

System code	Program office	System name	Acronym	Mission critical	Security financial PII	Type
(b)(5)						

Limitations

We noted no limitations to the accuracy, reliability, or validity of the evidence collected through our fieldwork process that was used to develop the findings and recommendations.

[15] FHA Catalyst Personal Identifiable Information Risk Management in a Zero Trust Environment (2023-OE-0007a)

APPENDIX C – SUMMARY OF CISA ZTA MATURITY RATINGS

Data Pillar

In assessing HUD's maturity level in the zero trust data functions, we rated four functions at the (b)(5) level and four at the (b)(5 level. We did not rate HUD at the (b)(5) or (b)(5) levels for any of the data functions, as shown in table 3.

Table 3: Enterprise data function rating matrix

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				

The average score for the data functions was midway between the (b)(5) levels, which indicated that HUD had implemented minimal controls to meet the zero trust data pillar requirements. HUD had strengthened its encryption capabilities, leveraged cloud technology to enhance redundancy and availability for many of its systems, improved its tools for visibility into its network and systems, and begun to automate several life cycle processes. However, HUD did not have a data inventory or data categorization structure, which are the building blocks of the data pillar, and which limited the usefulness of HUD's capabilities for visibility and analysis of its data. HUD also faced several challenges in the governance of its data program. For additional details on the maturity ratings, see table 4 below in which the boxes shaded green represent HUD's function rating.

Table 4: CISA ZTA maturity model – data pillar rating matrix

Function	1 - traditional	2 - initial	3 - advanced	4 - optimal
Data inventory management	(b)(5)			

Data categorization	(b)(5)
Data availability	
Data access	
Data encryption	
Visibility and analytics capability	
Automation and orchestration capability	
Governance capability	

Identity Pillar

In assessing HUD's maturity level in the zero trust identity functions, we rated two functions at the (b)(5) level, four at the (b)(level, and one at the (b)(5) level. We did not rate HUD at the (b)(5) level for any of the identity functions, as shown in table 5.

Table 5: Enterprise identity function rating matrix

Function	1 - traditional	2 - initial	3 - advanced	4 - optimal
Authentication	(b)(5)			
Identity stores				
Risk assessments				
Access management				
Visibility and analytics				
Automation and orchestration				
Governance				

The average score for the identity functions was just under the (b)(5) level, which indicated that HUD had only started to address the zero trust identity pillar requirements for some functions. This score reflects HUD's MFA initiative and the lack of a roadmap to implement further functions. The governance function was the (b)(5) rating because HUD established ICAM policies and procedures, including HUD's IT Security Control Catalog, and used CSAM to ensure that HUD has appropriate identity governance over program offices. HUD could improve the governance function by adding automation in identity governance over program offices. HUD could mature the other identity functions by starting with an updated roadmap to identify gaps and plan for budgeting and resource needs to move toward implementation. For additional details on the maturity ratings, see table 6 below, in which the boxes shaded green represent HUD's function rating.

Table 6: CISA ZTA Maturity Model – identity pillar rating matrix

Function	1 - traditional	2 - initial	3 - advanced	4 - optimal
Authentication	(b)(5)			
Identity stores				

Risk assessments	(b)(5)
Access management	
Visibility and analytics capability	
Automation and orchestration capability	
Governance capability	

APPENDIX D – LIST OF ABBREVIATIONS

Acronym	Definition
CDO	Chief Data Officer
CISA	Cybersecurity and Infrastructure Security Agency
CSAM	Cybersecurity Assessment and Management System
DHS	U.S. Department of Homeland Security
EA	Enterprise Architect
EO	executive order
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
HUD	U.S. Department of Housing and Urban Development
ICAM	identity, credential, and access management
IT	information technology
(b)(5)	(b)(5)
M	memorandum
MFA	multifactor authentication
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OFI	opportunity for improvement
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCIL	PII confidentiality impact level
PII	personally identifiable information
ZTA	Zero-trust architecture

APPENDIX E – 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