




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

HUD Fiscal Year 2024 Federal Information Security Modernization Act of 2014 Evaluation Report

Washington, DC | 2024-OE-0002


October 29, 2024



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.

Date: October 29, 2024

To: Adrienne Todman
Acting Secretary, S

From: Rae Oliver Davis 
Inspector General, G


Subject: Final Report – Fiscal Year 2024 Federal Information Security Modernization Act of 2014
Evaluation Report and Inspector General Metric Responses

We have completed our fiscal year (FY) 2024 Federal Information Security Modernization Act of 2014 (FISMA) evaluation. Our final report (FY 2024 FISMA Evaluation Report, Number 2024-OE-0002) and our responses to the annual Office of Inspector General (OIG) 2024 FISMA metrics are enclosed. FISMA requires Inspectors General (IG) to conduct an annual independent evaluation to determine the effectiveness of the agency information security (InfoSec) program and practices.

The Office of Management and Budget (OMB) established metrics for IGs to apply when conducting FISMA assessments. Consistent with OMB guidance, our evaluation assesses the Department's InfoSec program against these metrics to determine the maturity and effectiveness of the program. The domains are composed of 66 individual metrics, however, for FY 2024 OMB instructed IG's to focus the evaluation on 20 core and 17 supplemental metrics. The metrics and domains were assessed using a maturity model that is designed to measure the effectiveness of the agency's InfoSec program. Each domain is measured using a 5-level maturity model with maturity level 1 described as ad hoc and level 5 described as optimized. OMB and the OIG FISMA metric guidance states that an agency InfoSec program is effective at a maturity level 4, which is the managed and measurable maturity level. HUD's FY 2024 overall FISMA maturity was assessed at level 3, the "consistently implemented" maturity level, which increased from the FY 2023 maturity level. HUD increased in maturity for 22 metrics and maintained the same maturity for the remaining 15 metrics. Notably, HUD achieved maturity level 4, managed and measurable, for the first time in 14 metrics.

Our report highlights the initiatives to improve HUD's InfoSec program and improvements needed with associated recommendations to assist in addressing those weaknesses. We encourage HUD to continue the improvements, address our recommendations, and establish priorities to achieve an effective InfoSec program. We provide 5 new recommendations and 31 opportunities for improvement, with only the recommendations being formally tracked by our office. The report associates each FY 2024 HUD OIG recommendation to an IG FISMA metric. This association should enable HUD to better prioritize maturing each component of its InfoSec program. Further, each IG FISMA metric is supported by one or more Federal regulations, policies, guidance, or best business practices to guide HUD's improvement.

HUD's Office of the Chief Information Officer (OCIO)'s mission is to deliver technology solutions to support the customers' mission across the Department. OCIO collaborates with other HUD program offices to deliver these IT solutions and relies on consistent program office support to ensure a secure IT environment. OCIO had successes in many FISMA domains, including its data protection and privacy,



security training, incident response, and contingency planning programs. Significant challenges continued to impact the Chief Information Officer's (CIO) ability to establish an effective InfoSec program, notably in establishing its supply chain risk management program, executing configuration management initiatives, and managing and resourcing its identity, credential, and access management program.

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 will also be provided to congressional committees of jurisdiction and the U.S. Government Accountability Office as OMB and the Inspector General Act of 1978 require.

Enclosures:

Fiscal Year 2024 FISMA Evaluation Report (2024-OE-0002)

Cc: Gina Metrakas, Chief of Staff
Sairah Ijaz, Acting Chief Information Officer
Elizabeth de León Bhargava, Assistant Secretary of Administration
Vinay Singh, Chief Financial Officer
Damon Smith, General Counsel
Gayle Bohling, Deputy General Counsel for Operations
Juan Sargeant, Acting Deputy Chief Information Officer
Christina Addison, Acting, Chief Information Security Officer
David Peters, Chief Technology Officer
Michael Hill, Acting Assistant Chief Information Officer for Infrastructure and Operations
William Thompson, Assistant Chief Information Officer for Customer Relationship and Performance Management
Lori Sealy, Assistant Chief Information Officer for Business and IT Resource Management
Paul Scott, Business Change and Integration Officer
Porter Davis, Office of the Chief Information Officer Audit Liaison Officer
Natalia Vanegas, Acting Assistant Secretary for Public Affairs
Julia Gordon, Federal Housing Administration
Christopher Taylor, Field Policy and Management National Director

This page intentionally left blank

Executive Summary

FISCAL YEAR 2024 FISMA EVALUATION REPORT | 2024-OE-0002

Purpose

We evaluated the U.S. Department of Housing and Urban Development’s (HUD) information security (InfoSec) program in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), which directs Inspectors General (IG) to conduct assessments using the IG FISMA metrics. The Office of Management and Budget (OMB) issued the fiscal year (FY) 2024 IG FISMA metrics, which consisted of nine domains aligned with the five functional areas from the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity. A total of 37 metrics were evaluated in FY 2024, which included both 20 core metrics that are assessed annually and 17 FY 2024 supplemental metrics that are assessed every other year.

Our objective was to assess the effectiveness of HUD’s InfoSec program on a maturity model in accordance with FISMA requirements. Each function, domain, and metric were measured using a five-level maturity model with maturity level 1 representing ad hoc and maturity level 5 representing optimized. OMB and IG FISMA metric guidance state that an InfoSec program is effective at maturity level 4, managed and measurable.

Findings

HUD continued to take positive steps to improve its information technology (IT) security posture. HUD improved its InfoSec program to maturity level 3, consistently implemented. However, at this level HUD’s InfoSec program is not considered effective. HUD’s InfoSec program scored a 3.08 for the core metrics and a 3.30 for the FY 2024 supplemental metrics,¹ both of which were at maturity level 3, consistently implemented. HUD increased in maturity for 22 metrics and maintained the same maturity for the remaining 15 metrics. Notably, not only did HUD achieve maturity level 4, managed and measurable, for the first time and it did so in 14 metrics. HUD also continued to make significant progress in addressing our prior years’ recommendations. During FY 2024, HUD closed 34 recommendations. A summary of HUD’s maturity level distribution is provided in figure 1.

¹ [Final FY 2023 - 2024 IG FISMA Reporting Metrics v1.1 \(cisa.gov\)](https://www.cisa.gov)

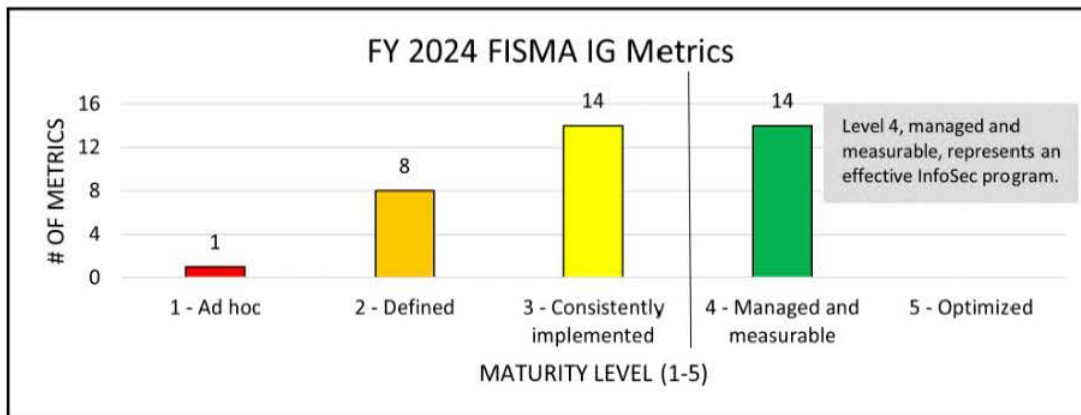



Figure 1. HUD maturity level distribution

HUD made commendable progress on increasing maturity for 22 metrics and should continue to focus on prioritizing maturity in the 20 core metrics and key cyber executive orders and requirements outlined below. These efforts will require a shared responsibility of proper resourcing, planning, and support from all levels of leadership across the Department.

HUD’s Office of the Chief Information Officer’s (OCIO) mission is to deliver technology solutions to support the customers’ mission across the Department. OCIO collaborates with other HUD program offices to deliver these IT solutions and relies on consistent program office support to ensure a secure IT environment. OCIO had successes in many FISMA domains, notably reaching the managed and measurable maturity level for its data protection and privacy, security training, incident response, and contingency planning programs.

HUD’s successes in FY 2024 were attributed to implementing technology solutions, implementing performance measures, and resource and personnel allocation. HUD’s implementation of a Continuous Diagnostics and Monitoring (CDM) dashboard improved its InfoSec maturity in several areas. First, the CDM dashboard gave HUD better visibility of its system, hardware, and software inventories. Second, the CDM dashboard provided HUD with an overview of its identified security weaknesses, including both configuration issues and software vulnerabilities. In addition, HUD’s information security continuous monitoring (ISCM) program used the System Security Dashboard, which helped HUD collect, analyze, and report on agency data in a timely manner with the goal of managing risk as appropriate, based on the organization’s core missions and business processes. HUD’s incident response program also used new solutions, such as a security incident event management tool, to monitor its network. This tool provided Security Operations Center (SOC) analysts with insights that were used to collect data to analyze incidents and perform triage. In maturing its incident response program, HUD continued to strengthen its data exfiltration and network defenses. The SOC upgraded its detection and protection tools for monitoring inbound and outbound network traffic and enhanced its technical capabilities for detecting anomalous traffic patterns and elements of personally identifiable information.

In FY 2024, HUD increased in maturity in four of the nine domains to the managed and measurable maturity level, which demonstrated an effective InfoSec program. To reach this maturity level, several metrics within these domains required performance measures to be monitored, analyzed, and reported to stakeholders to make improvements to the program. HUD implemented performance measures to



capture data on its incident response capability. HUD monitored and analyzed qualitative and quantitative performance measures to monitor and improve the effectiveness of its overall incident response capability, including mean time to detect incidents, mean time to identify, and mean time to recover. These measures also accounted for privacy incidents, as well as the timeliness of the SOC in notifying stakeholders such as the Privacy Team. The incident response and data protection performance measures also help inform HUD's security training program, in which HUD users may need additional training and information on certain attack vectors. HUD implemented monthly phishing exercises for all users and captured metrics on these exercises to inform and improve the program.

Lastly, personnel and resource allocation were key to maturing an effective InfoSec program. The Privacy Office conducted an analysis of its current resources and determined the additional staffing and skills needed to meet privacy program requirements and objectives. In FY 2024, HUD began to add resources and address some of these gaps, which contributed to the privacy program's ability to improve its data protection and privacy capabilities. Another example of how personnel and resource allocation led to an improved capability is HUD's ISCM and ongoing authorization (OA) program. During FY 2024, HUD continued its enrollment of systems into the ISCM and OA program in the implementation phase, and HUD onboarded contractor support to perform OA assessments.


Although HUD had many successes in FY 2024, it also had challenges that limited its ability to mature in key InfoSec areas, notably in establishing its supply chain risk management (SCRM) program and managing and resourcing its identity, credential, and access management (ICAM) program.

HUD was still establishing its SCRM program, including developing a strategy, policies, and procedures, late in FY 2024. Establishing the program would support an IT acquisition program that monitors and manages risk to acquisition of a diverse range of IT products and services needed by HUD to accomplish its mission. Acquisition of IT products and services involves complex, globally distributed supply chains with multiple layers of outsourcing.

HUD's ICAM program is designed to ensure that only authorized users and devices can access HUD's IT systems and sensitive data. By implementing strong controls in this domain, HUD can minimize opportunities for adversaries to compromise user accounts, gain a foothold in systems, steal data, or launch cyberattacks. As technology moved towards more secure methods of access and authorization, HUD continued to lack multifactor authentication (MFA) but implemented a pilot program funded by the Technology Modernization Fund. In compliance with provisions of Executive Order 14028 and related implementing guidance within OMB Memorandum (M)-22-09, agencies are required to progress toward a zero-trust architecture by integrating MFA at the application level and deemphasizing network-level authentication. MFA provides an additional layer of identity verification compared to a password alone, significantly improving information system security.

Although we determined HUD had an effective incident response program in FY 2024, HUD still needs to meet the event-logging requirements in accordance with OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.

HUD's OCIO should continue addressing open recommendations from previous FISMA evaluations, specifically recommendations to increase maturity in the core metrics; develop, modernize, and enhance



its legacy systems; strategically utilize its resources, including staff and funding; and deploy technology necessary to implement critical security controls.

Recommendations

In this report, we offer five new recommendations and offer opportunities for improvement (OFI) for the enterprise and program offices. These OFIs will not be tracked as formal recommendations but are noted as general suggestions for HUD to improve the effectiveness of its InfoSec program implementation. The recommendations should help HUD improve in several InfoSec areas, including its inventory of assets, governance, risk, and compliance, security configuration of its systems, including baseline configurations, and security training improvements.

Table of Contents

Executive Summary	6
Introduction	11
Background	11
IG FISMA Metrics	12
FY 2022 Through FY 2024 FISMA Cycle	14
Objective	14
Results of Review	15
Summary and Overall FY 2024 Maturity Level.....	15
Spotlights on Key Initiatives	16
Program Improvement Needs	19
HUD’s IT Budget	25
Conclusion	26
Recommendations	28
Appendixes	29
Appendix A – Agency Comments and OIG’s Response	29
Appendix B – Scope, Methodology, and Limitations	31
Appendix C – Summary of Prior FISMA Recommendations	36
Appendix D – Opportunities for Improvement.....	38
Appendix E – List of Abbreviations	41
Appendix F – FY 2024 HUD OIG CyberScope Submission	43
Appendix G – HUD FISMA Metric Trends.....	44
Appendix H – Acknowledgements	49

Introduction

BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) requires all Inspectors General (IG) to annually assess the effectiveness of their Federal agency's information security (InfoSec) programs. The Office of Management and Budget (OMB) publishes metrics annually for the IG community to use during these assessments in the form of a maturity model.

IGs are required to submit the results of their FISMA assessments to OMB and the U.S. Department of Homeland Security (DHS) through the DHS-hosted CyberScope portal, which is structured to allow individual responses to each metric within a domain. Consistent with OMB guidance, the U.S. Department of Housing and Urban Development's (HUD) Office of Inspector General (OIG) has elected to provide an additional narrative report summarizing the results of our FISMA assessment and provide recommendations and opportunities for improvement (OFI). These recommendations and OFIs can assist HUD to prioritize maturing components within its InfoSec program.

FISMA Overview

The Federal Information Security Management Act of 2002,² as amended by FISMA,³ establishes the following responsibilities for agency heads:

- providing InfoSec protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- ensuring compliance with the requirements of FISMA; OMB policies; and National Institute of Standards and Technology (NIST) policies, procedures, standards, and guidelines;
- ensuring that InfoSec management processes are integrated with agency strategic and operational planning processes;
- ensuring that senior agency officials provide InfoSec for the information and information systems that support the operations and assets under their control; and
- ensuring that all personnel are held accountable for complying with the agencywide InfoSec program.

FISMA also requires each agency OIG to conduct an annual independent evaluation to determine the effectiveness of the InfoSec program and practices of its respective agency. Additionally, Offices of the Chief Information Officer (OCIO) are required to submit Chief Information Officer (CIO) metrics quarterly, which are also organized around NIST security guidelines. In accordance with the Administration's shift in InfoSec focus, the fiscal year (FY) 2024 CIO metric responses should reflect the implementation of

² [Public Law No. 107-347, Title III, Federal Information Security Management Act of 2002 \(Dec. 2002\)](#)

³ [Public Law No. 113-283, Federal Information Security Modernization Act of 2014 \(Dec. 2014\)](#)

cybersecurity-related initiatives, including those in support of Executive Order 14028, Improving the Nation’s Cybersecurity.⁴

IG FISMA METRICS

OMB’s Office of the Federal CIO issued the FY 2023-2024 IG FISMA Reporting Metrics on February 10, 2023.⁵ The 66 metrics in this document were separated into 4 categories, as detailed below:

- 20 core metrics, which are intended to be assessed annually.
- 20 FY 2023 supplemental metrics, which are intended to be assessed every other year beginning in FY 2023.
- 17 FY 2024 supplemental metrics, which are intended to be assessed every other year beginning in FY 2024.
- Nine optional domain summary metrics, which OIGs may use to report additional information for each domain.

We evaluated the 20 core metrics and the 17 FY 2024 supplemental metrics according to the OMB guidance, above. HUD OIG does not generally use the nine optional domain summary metrics. In total, 37 of the 66 metrics were assessed in this evaluation, in accordance with OMB guidance.

Metric and Domain Alignment to the NIST Cybersecurity Framework

Since FY 2016, the IG FISMA metrics and the nine FISMA domains have been aligned to the five function areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF),⁶ which are as follows: identify, protect, detect, respond, and recover. Table 1 shows how the nine FISMA domains are aligned to the five NIST CSF function areas.

Table 1. FISMA domain alignment to the NIST CSF function areas

NIST CSF function	FISMA domains
Identify	<ul style="list-style-type: none">▪ Risk management▪ Supply chain risk management
Protect	<ul style="list-style-type: none">▪ Configuration management▪ Identity and access management▪ Data protection and privacy▪ Security training
Detect	<ul style="list-style-type: none">▪ Information security continuous monitoring
Respond	<ul style="list-style-type: none">▪ Incident response
Recover	<ul style="list-style-type: none">▪ Contingency planning

⁴ [OMB M-24-04, FY 2024 Guidance on Federal Information Security and Privacy Management Requirements](#)

⁵ [FY 2023 - 2024 IG FISMA Reporting Metrics](#)

⁶ [Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1](#)

IG FISMA Core Metrics

The 20 core metrics that were selected by OMB beginning in FY 2022 represent a combination of Administration priorities, high-impact security processes, and essential functions necessary to determine overall InfoSec program effectiveness. The core metrics were primarily chosen to align with Executive Order 14028.⁷ Additional OMB cybersecurity guidance that aligns with the core metrics includes

- Memorandum (M)-21-31, Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents
- M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response
- M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

Metric Maturity Model

The IG FISMA metrics use a five-level maturity model for each domain and NIST CSF function, establishing criteria to determine the level of maturity. According to OMB and DHS guidance, maturity level 4—managed and measurable—represents an effective level of security, as shown below in figure 2.⁸ The maturity levels for the five NIST CSF functions together measure the overall InfoSec program effectiveness.



Figure 2. IG FISMA maturity model levels

⁷ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

⁸ [Security and Privacy Controls for Information Systems and Organizations \(nist.gov\)](https://www.nist.gov/privacy-security) defines security and privacy control effectiveness and addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the designated security and privacy requirements.

FY 2022 THROUGH FY 2024 FISMA CYCLE

FY 2024 concluded a 3-year cycle in which IGs were required to evaluate all 66 metrics. HUD made continued improvements in this 3-year cycle, culminating in an increased maturity level in FY 2024. All agencies report on IG metrics annually through an assessment conducted by the agency IG or an independent assessor. To help facilitate this, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) transitioned the IG metrics process to a multiyear cycle. OMB selected a core group of metrics, representing a combination of Administration priorities and high-impact controls, that must be evaluated annually. The remainder of the standards and controls were evaluated on a 2-year cycle starting in FY 2023 as supplemental metrics.

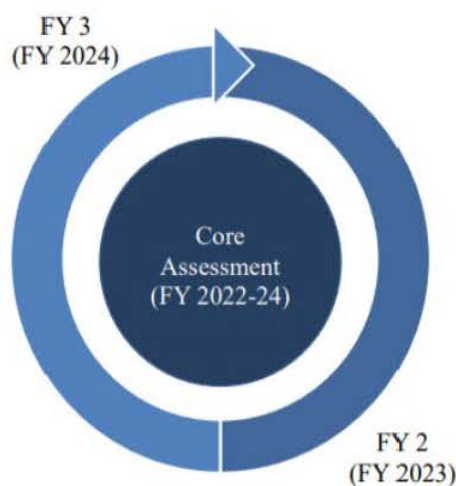
In FY 2022, OMB and CIGIE issued 20 core metrics to be assessed annually. HUD's InfoSec program was determined to be at the defined maturity level, which was considered not effective, based on our evaluation of these 20 core metrics, scoring a 2.37. HUD had generally achieved a higher maturity level in the supplemental metrics in previous evaluations. Therefore, the exclusion of the supplemental metrics affected the rating of HUD's overall InfoSec program and maturity level.

In FY 2023, we evaluated the 20 core metrics and 20 supplemental metrics and concluded that HUD continued to take positive steps to improve its information technology (IT) security posture.

However, based on the FY 2023 IG FISMA metrics issued by OMB and CIGIE, HUD's InfoSec program was at level 2, defined, which is a level that was considered not effective. HUD's InfoSec program scored 2.60 for the 20 core metrics, an improvement from FY 2022. Additionally, HUD scored a 2.86 for the FY 2023 supplemental metrics. HUD made commendable progress on increasing maturity in 10 metrics and achieved level 4, managed and measurable, maturity level for the first time in 2 metrics. Although HUD improved overall, four of the five metrics in which HUD dropped in maturity were core metrics, in which HUD should continue to focus on prioritizing maturity to address Administration priorities and high impact controls.

OBJECTIVE

The objective of this evaluation was to assess the maturity level of HUD's InfoSec program and practices in accordance with the IG FISMA metrics. Our fieldwork and evaluation procedures enabled us to respond to the Annual IG Report in the DHS CyberScope reporting database and prepare this FY 2024 FISMA evaluation narrative report. Appendix B describes the scope and methodology used to complete the evaluation.



Results of Review

SUMMARY AND OVERALL FY 2024 MATURITY LEVEL

In FY 2024, HUD continued to take positive steps to improve its IT security posture. However, based on our evaluation of the 20 core metrics and 17 supplemental metrics, HUD’s InfoSec program was evaluated as maturity level 3, consistently implemented, which was considered not effective. HUD’s overall InfoSec program scored a 3.08 in the core metrics and a 3.30 in the FY 2024 supplemental metrics, which both represent increases in maturity from previous years. HUD made steady improvements in the core metrics over the 3-year FISMA cycle from FY 2022 through FY 2024, as shown in figure 3 below. HUD should continue to focus on prioritizing maturity in the 20 core metrics and key cyber executive orders and requirements. These efforts will require a shared responsibility of proper resourcing, planning, and support from all levels of leadership across the Department.

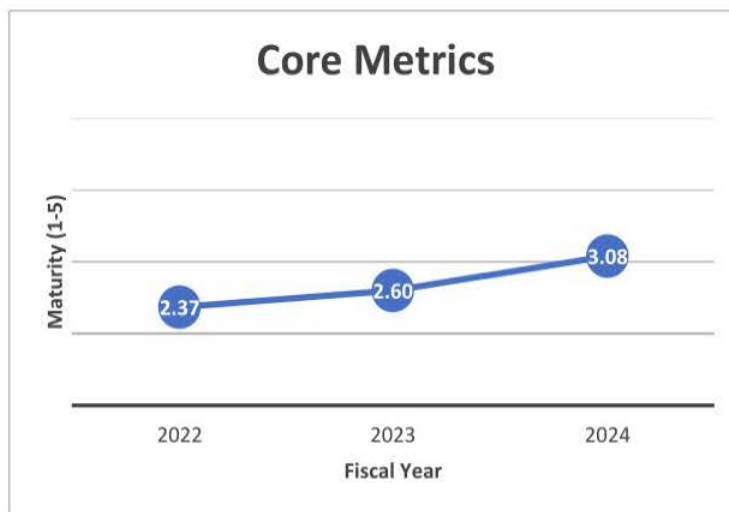


Figure 3. Core metric scoring progression

HUD made significant improvements in metrics across all domains, maturing in 22 of the 37 that were evaluated. HUD improved in three of five functions, reaching the managed and measurable level of maturity for the respond and recover functions and the consistently implemented level for the protect function. HUD’s achievement of reaching the managed and measurable maturity level in the respond and recover functions represented an effective level of maturity in a function for the first time. HUD remained at the same level of maturity for two of five functions, with the identify function maintaining the defined level of maturity and the detect function maintaining the consistently implemented level of maturity.

However, HUD continued to show limitations in establishing its supply chain risk management (SCRM) program and managing and resourcing its identity, credential, and access management (ICAM) program. HUD OCIO should continue addressing open recommendations from previous FISMA evaluations; develop, modernize, and enhance its legacy systems; strategically utilize its resources, including staff and funding; and deploy technology necessary to implement critical security controls. We summarized key results from the metric assessment in this report. See table 2 for HUD’s maturity level in

each domain, function, and overall InfoSec program in FY 2024. Please see appendix F for the full CyberScope report and appendix G for a summary of HUD’s metric maturity trends since FY 2022.

Table 2. FISMA domain, NIST CSF function, and overall InfoSec program maturity

Domain	Maturity level	Function	Overall InfoSec program
Risk management	3 – consistently implemented	2 – defined (identify)	3 – consistently implemented
Supply chain risk management	2 – defined		
Configuration management	3 – consistently implemented	3 – consistently implemented (protect)	
Identity and access management	2 – defined		
Data protection and privacy	4 – managed and measurable		
Security training	4 – managed and measurable	3 – consistently implemented (detect)	
Information security continuous monitoring	3 – consistently implemented		
Incident response	4 – managed and measurable	4 – managed and measurable (respond)	
Contingency planning	4 – managed and measurable	4 – managed and measurable (recover)	

SPOTLIGHTS ON KEY INITIATIVES


Implementation of Technology Solutions

CDM Dashboard

HUD’s implementation of a Continuous Diagnostics and Monitoring (CDM) dashboard improved its InfoSec maturity in several areas. First, the CDM dashboard gave HUD better visibility of its system, hardware, and software inventories. Having an accurate picture of its system, hardware, and software inventories is foundational to other areas of the InfoSec program, such as configuration management, ICAM, data protection and privacy, information security continuous monitoring (ISCM), incident response, and contingency planning, because those areas depend on an accurate inventory for effective program operations.

Second, the CDM dashboard provided HUD with an overview of its identified security weaknesses, including both configuration issues and software vulnerabilities. These weaknesses were assigned a score based on the criticality of the risk, which helped HUD prioritize the most significant threats to its InfoSec resources.

HUD’s CDM dashboard is a significant improvement to its overall maturity. However, HUD will need to continue to maintain and improve the CDM dashboard to have an effective InfoSec program. The CDM dashboard is an ongoing monitoring process, and if HUD does not prioritize its resources to continue updating the CDM dashboard, it could lose the improvements in maturity it has made in this area. For example, this happened in previous years with the System Security Dashboard, discussed below. Like the



CDM dashboard, the System Security Dashboard was updated in FY 2024. However, this remains an area for HUD to prioritize its resources towards. Without timely updated information, HUD cannot make prioritized decisions about what threats need to be addressed first. In addition, the CDM dashboard in its current form, does not address all the criteria in the inventory and scanning metrics, as discussed below in the Program Improvement Needs section.

System Security Dashboard


A comprehensive ISCM strategy is key to maintaining ongoing awareness of information security, vulnerabilities, and threats to support organization risk management decisions. HUD's ISCM program implemented a tool called the System Security Dashboard and strategies for assessments of system controls and all other FISMA activities. This tool helped HUD collect, analyze, and report on agency data in a timely manner with the goal of managing risk as appropriate, based on the organization's core missions and business processes. Data points and metrics were established in the System Security Dashboard via results of the security and privacy control assessments to measure the performance of each system enrolled in the ISCM program. The System Security Dashboard also provides insight into the performance of the ISCM program itself; for example, the total systems onboarded into the program and their security posture. HUD continued to enroll systems in its ISCM and ongoing authorization (OA) program in FY 2024. This program aimed to achieve visibility into the security of HUD's IT assets, awareness of cybersecurity risk, and insight into the effectiveness of deployed security and privacy controls.

Incident Response and Privacy Capabilities

HUD also continued to improve its incident response program in FY 2024. An effective incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction of data, mitigating the weaknesses that were exploited, and restoring IT services.⁹ Potential incidents must be detected then analyzed to determine proper communication and response actions from the appropriate stakeholders in accordance with key Administration priorities as outlined in Executive Order 14028. Appropriate tools and technologies must be employed to resolve incidents in a timely manner, which requires a fully operational Security Operations Center (SOC). In FY 2024, HUD used a security incident event management (SIEM) tool to monitor its network, ingesting information from on-premises systems and several cloud service providers and working toward onboarding several more. HUD's SIEM capability matured in FY 2024, which provided SOC analysts with insights that were used to create tickets and perform incident triage. However, HUD was still onboarding web applications into its new SIEM to provide more visibility of those systems.

In maturing its data protection and privacy program, HUD continued to strengthen its data exfiltration and network defenses. The SOC upgraded its detection and protection tools for monitoring inbound and outbound network traffic and enhanced its technical capabilities for detecting anomalous traffic patterns and elements of personally identifiable information (PII). HUD participated in the Cybersecurity and Infrastructure Security Agency (CISA) analysis process to review available products to cover the gaps that existed in its defenses and selected an upgraded endpoint detection and response (EDR) solution based upon that assessment. The EDR solution enabled the SOC to better monitor user activity on its endpoints

⁹ [Computer Security Incident Handling Guide \(nist.gov\)](https://www.nist.gov/cybersecurity/incident-handling-guide)



and to identify and protect sensitive data including PII. The solution further supported threat hunting, alert triage, and user activity validation.¹⁰ In FY 2024, the SOC added file integrity monitoring and forensics components to its EDR suite and was baselining another product to provide user behavior analytics to further improve detections of anomalous activity by its users.

Implementation of Performance Measures

In FY 2024, HUD increased in maturity in four of the nine domains to the managed and measurable maturity level, which demonstrated an effective InfoSec program in those domains. To reach this maturity level, several metrics within these domains required performance measures to be monitored, analyzed, and reported to stakeholders to make improvements to the program. HUD's System Security Dashboard captured performance measures across different areas of its InfoSec program. Some of these performance measures included authorization to operate (ATO) compliance, plans of actions and milestones (POA&M) tracking, privacy compliance, and contingency planning efforts. These are critical for HUD to have full visibility into system weaknesses and to ensure that the systems are operating effectively.

Incident Response and Privacy Metrics

HUD also implemented performance measures to capture data on its incident response capability. HUD monitored and analyzed qualitative and quantitative performance measures to monitor and improve the effectiveness of its overall incident response capability. HUD defined the metrics in its incident response plan, and the metrics were collected and analyzed through its SIEM tool. Some metrics included mean time to detect incidents, mean time to identify, and mean time to recover. The data also captured the types of alerts generated, such as unauthorized access, large web uploads, and other malicious activity.

The data protection and privacy program supported the incident response capability with measures to assess the effectiveness of its data breach response plan. Quantitative measures focused on privacy incident detection and response timeliness, while qualitative measures focused on response thoroughness and compliance with requirements. These measures complemented the incident response measures which assessed the effectiveness of the SOC in responding to privacy incidents and notifying stakeholders such as the Privacy Team. The data breach response plan required team meetings after major incidents and periodically after lesser incidents to identify lessons learned and drive improvement to its processes and performance measures.

Security Training Metrics

The incident response and data protection performance measures also help inform HUD's security training program, in which HUD users may need additional training and information on certain attack vectors. HUD's security training program encompassed both general awareness training for all users and specialized, role-based training for individuals with specific IT security responsibilities. Those who use or manage HUD's IT systems should fully understand their security responsibilities, be able to recognize

¹⁰ Although HUD improved their capabilities, the FY 2024 penetration test evaluation (2024-OE-0002a) found some weaknesses. We will continue to review this capability in future evaluations.

common attack vectors, and know how to respond to incidents. Because system users can pose a significant risk to IT security, technical measures alone are insufficient to protect against evolving threats.

A robust security and awareness training program can help to establish a strong culture of cybersecurity and contribute to the broader objective across all FISMA domains for safeguarding the confidentiality, integrity, and availability of HUD's information and information systems. HUD continued to improve its security training program, reaching the managed and measurable maturity level in FY 2024. HUD implemented monthly phishing exercises for all users. If a user clicks on the phishing link, they are directed to HUD's Office of the Chief Information Security Officer (OCISO) homepage for additional guidance and training. HUD captured metrics on the phishing exercises to inform and improve the program. The phishing metrics include who clicked on the link and who reported the phishing appropriately. These results were collected at the program office level and aggregated at the HUD level, rolled into an after-action report to the Chief Information Security Officer, and discussed at monthly information system security officer forums.

Personnel and Resource Allocation

Privacy Office Resources

In FY 2023, the Privacy Office conducted an analysis of its current resources and determined the additional staffing and skills needed to meet privacy program requirements and objectives. In FY 2024, HUD began to add resources and address some of these gaps, which contributed to the privacy program's ability to improve its data protection and privacy capabilities. These additional resources enabled the privacy program to improve its data breach response capability, improve its privacy training program, and better integrate its process with the SOC to support functions such as incident response, data monitoring, and endpoint detection and response.

ISCM Assessment Program

Another example of how personnel and resource allocation led to an improved capability is HUD's ISCM and OA program. During FY 2024, HUD continued its enrollment of systems into the ISCM and OA program, and HUD onboarded contractor support to perform OA assessments. Additionally, HUD continued developing its System Security Dashboard using contractor support. This provided HUD a clear view of vulnerabilities, up-to-date threat information, and related mission impacts for systems enrolled in the ISCM program. The dashboard includes summary information related to ATO artifact compliance, POA&M management, and ISCM security control assessment results.

PROGRAM IMPROVEMENT NEEDS

Identity, Credential, and Access Management

Multifactor Authentication

ICAM processes are designed to ensure that only authorized users and devices can access an organization's IT systems and sensitive data. In today's cyber threat landscape, usernames and passwords are no longer a secure method of authentication, and use of this authentication method puts the agency at risk for an adversary to access sensitive information, perform data exfiltration, launch or further attacks. By implementing phishing-resistant multifactor authentication (MFA), HUD can minimize

opportunities for adversaries to compromise user accounts, gain a foothold in systems, steal data, or launch cyberattacks.

HUD made limited progress in the ICAM domain by defining a plan to implement phishing-resistant MFA to all privileged and non-privileged users accessing HUD systems. HUD established an MFA deployment plan with milestones that it began to implement. HUD used the Technology Modernization Fund (TMF) award to support the pilot of the MFA solution identified. While HUD established a plan for MFA, HUD had not met the OMB M-22-09 requirement for implementation of MFA for all public-facing systems by January 2023, and HUD did not reach full implementation by the end of FY 2024.¹¹ Additionally, HUD faced challenges with the MFA rollout due to determining a practical MFA solution that best meets the needs of the clientele HUD serves. Lastly, HUD made no improvement in MFA access to facilities, as it does not have a plan to establish MFA for physical access, which is an open recommendation from the FY 2023 FISMA evaluation.

User Logging Requirements

User logging is an additional area of ICAM in which HUD did not mature during FY 2024. Logging increases visibility of user actions and helps system administrators ensure that user activity within a system is normal. OMB M-21-31 established a four-tier maturity model (not effective, basic, intermediate, and advanced) to categorize agency logging capabilities and required that Federal agencies achieve all four levels by September 2023.¹² HUD planned to reach basic (EL1) logging capabilities by March 2024, but had onboarded only (b)(5) applications and had not met its EL1 milestone. HUD also planned to reach intermediate (EL2) logging capabilities by June 2024 but did not meet this milestone. Until HUD increases logging capabilities, it could be difficult to identify discrepancies or potential attacks.

Implementing Executive Order 14028 Requirements

Zero Trust Architecture

In 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 14028 stressed the critical need for a zero trust architecture (ZTA) to protect critical data. In support of Executive Order 14028, CISA issued a maturity model to measure agency progress in five pillars (identity, devices, networks, applications and workloads, and data), as shown in figure 4 below. OMB M-22-09 subsequently set forth a Federal ZTA strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of FY 2024 to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns.

¹¹ [OMB M-22-09 Federal Zero Trust Strategy](#)

¹² [OMB M-21-31 Improving the Federal Government's Investigation and Remediation Capabilities Related to Cybersecurity Incidents](#)



Figure 4. CISA zero trust maturity model pillars evolution

On April 4, 2022, HUD issued its Zero Trust Strategy Implementation Plan, which identified data protection as the most critical element HUD would prioritize for zero trust. HUD identified specific data pillar actions to address the OMB requirements; however, this plan did not address data categorization and security response requirements and identified significant budget and resource challenges to meeting the data logging requirements.

Since issuance of this plan, HUD has shifted its focus to the identity pillar requirements and secured an enterprise-wide identity management tool. HUD was in the initial stages of implementing phishing-resistant MFA through this tool and planned to use the tool for enterprise identity management purposes to meet zero trust requirements. HUD established a plan for the other three zero trust pillars (devices, networks, and applications and workloads) and addressed some of the tasks it self-identified; however, HUD has not yet addressed all areas within the five pillars. The shift in prioritization from the data to identity pillar and HUD's challenges in completing its self-identified tasks indicate that HUD's Zero Trust Strategy Implementation Plan is not sufficient in addressing how HUD will implement zero trust requirements.

Critical Software

HUD had not updated its inventory policies and procedures to include critical software and critical software platforms as required by Executive Order 14028. We issued recommendations in FY 2023 to address these Executive Order 14028 requirements. As defined by NIST and CISA, critical software is any software that runs with elevated privileges or manages privileges; has privileged access to network or computing resources; controls access to data or operational technology; performs a critical trust function, such as network control, protection, or endpoint security; or operates outside the agency's normal trust

boundaries.¹³ In particular, this definition of critical software is not directly related to HUD's determination of its high-value assets (HVA) or mission essential functions (MEF).

As a result, HUD did not have visibility into which of its systems, if any, would be considered critical software platforms. This lack of awareness also prevented HUD from being able to effectively enforce the requirements to keep all software on systems that are critical software platforms updated to supported versions. HUD's general policy for software versions allows the use of supported versions or one previous version, but this is not sufficient to meet the requirements for critical software platforms under Executive Order 14028.

Policies, Procedures, and Governance

Supply Chain Risk Management

HUD released its SCRM policies and procedures in late FY 2024; however, HUD remained at an ineffective maturity level in the SCRM domain. Supply chain risk affects many parts of the InfoSec program, so this is an area in which HUD should focus on improving its maturity. For example, systems operated internally by HUD could be vulnerable to supply chain threats from counterfeit components or a lack of available replacement components. Similarly, systems operated external to HUD, such as cloud systems, face the same supply chain threats. External systems also need to be verified for compliance with HUD's security policies, because HUD does not directly control these external systems.

Configuration and Vulnerability Scanning

HUD's defined procedures for configuration and vulnerability scanning required systems to be scanned every 14 days. In practice, HUD showed that scans were generally occurring every 3 days (72 hours), with some scans being scheduled for 2 times per week. HUD should align its scanning policies and procedures with its chosen implementation, preferably by defining a scanning timeline of less than 14 days. In addition, HUD's scanning policies and procedures exempt web applications from the 14-day scanning requirement. Web applications are required to be scanned once per year, instead of the more frequent requirements for other systems.


Web Application Inventory

HUD had a conflict between two separate policies and procedures for its web application inventory. The Inventory of Automated Systems (IAS) policy required HUD to maintain a single inventory for all systems, including web applications. The web applications inventory policy stated that web applications would be maintained in a separate single inventory in a SharePoint site. Both policies cannot be met unless the single inventory is in IAS. This is representative of HUD's issues with maintaining consistent policies and procedures and implementing processes in accordance with those policies and procedures.

Governance, Risk, and Compliance Tool

HUD reported that it implemented a governance, risk, and compliance (GRC) tool in its CIO metrics. However, HUD still has an open recommendation from the FY 2021 FISMA evaluation to use the GRC tool

¹³ [Definition of Critical Software Under Executive Order 14028](#)



to manage all risk information across all three tiers of the organization.¹⁴ Further, HUD needs to implement an automated GRC tool to improve its maturity. A GRC tool will provide information to stakeholders to make informed decisions, but the tool is only as useful as the information that it consumes. If HUD's GRC tool does not include all risk information from all tiers, stakeholders making decisions will not have full visibility. Stakeholders may think that they are making their decisions based on all available information when they are not doing so, because the GRC tool is not providing all available information. Automation is also important for an effective GRC tool to keep the information that is provided updated in a timely manner.

Security Training of External Users

Although HUD made major improvements to its security training program, it still lacked the process to provide training to all users of HUD data. NIST Special Publication (SP) 800-50 defined that users are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, other agency personnel, visitors, guests, and other collaborators or associates requiring network access. Users must understand and comply with agency security policies and procedures, be appropriately trained in the rules of behavior for the systems and applications to which they have access, and work with management to meet training needs. HUD required its employees and contractors to take general cybersecurity awareness training annually. Other collaborators, referred to as external users, such as public housing agency employees, were only required to sign a Rules of Behavior for the systems they accessed. External entities attest as part of the memorandum of understanding/interconnection security agreement template that external users have completed the required organizational security training. HUD does not directly provide cybersecurity training to external users.


Business Impact Analysis

HUD improved its contingency planning efforts, including contingency plan testing. However, we found inconsistencies with the business impact analysis (BIA) process. The BIAs capture a weighted combination of the recovery time objective, recovery point objective, and maximum tolerable downtime from each system BIA to prioritize the recovery order of its systems. The information from the system-level BIAs was consolidated into an enterprisewide business impact analysis (EWBIA) as defined in HUD's policy. It included determination of mission and business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. HUD planned to conduct another EWBIA in FY 2025. HUD did not use the results of the BIA consistently to determine contingency planning requirements and priorities, including MEFs and HVAs. HUD has an open recommendation from the FY 2022 FISMA evaluation for HUD OCIO and the Office of Administration to coordinate the list of systems prioritized by the EWBIA with the list of MEFs and HVAs.

Trusted Internet Connection

Last, HUD's Trusted Internet Connection (TIC) program had not been updated from TIC 2.0 to TIC 3.0, which was recommended during the FY 2021 FISMA evaluation. An agency's TIC program is the process by which it ensures that network traffic is protected. TIC 3.0 expands the types of connections that an

¹⁴ The three tiers are enterprise level; mission/business process level or program office level; and system level.



agency may consider in its network setup, which are called “use cases.” For example, remote employees may not have their network traffic sent through HUD’s on-premise network directly, but this traffic still needs to be secured. Agencies were required to move to TIC 3.0 by September 12, 2020.¹⁵ In FY 2023, HUD showed that it was considering two use cases under the TIC 3.0 program.

¹⁵ [OMB M-19-26 Update to the Trusted Internet Connections Initiative](#)

HUD'S IT BUDGET

Although not specifically required by OMB's FISMA criteria, we reviewed HUD's IT budget because its available resources impact the implementation of the InfoSec program. OCIO's IT fund has a significant influence on its InfoSec program maturity because of the need to use sufficient resources to procure and implement cybersecurity tools and technologies. HUD has reported that IT funding and resources have historically been a cybersecurity concern. As HUD continues to mature its InfoSec program, more technologies, capabilities, and system modernization are required to meet Administration priorities and increase the maturity of HUD's InfoSec program. HUD's limited resources have been a factor in contract lapses, with OCIO reporting the reduction or elimination of various operations and maintenance (O&M) services in previous years. When resourcing issues occur, OCIO reportedly (b)(5)

(b)(5)

(b)(5)

HUD was able to restore funding for these services in FY 2024. However, HUD will need to support more IT areas as its maturity increases. Supporting a ZTA, the implementation of MFA, the maturation of the SCRM program, and the implementation of its planned GRC tool will all require additional resources in future years.

Most of the IT funds OCIO received were used to maintain ongoing O&M of legacy systems, which have a high annual cost. This need for O&M has contributed to HUD's inability to develop, modernize, and enhance its IT environment, leaving large numbers of legacy systems in operation. These systems continue to elevate risks to HUD's IT environment, are resource intensive, and limit the effectiveness of OCIO to acquire and deploy technology necessary to implement critical security controls and modernize.

HUD received \$383.05 million for the FY 2024 IT Fund to support the O&M of current systems and limited development, modernization, and enhancement (DME) of new initiatives. This is an increase of \$8.3 million in funding compared to FY 2023, and the increase is intended to support new cybersecurity initiatives. Of the \$383.05 million in the IT Fund, \$29.35 million was earmarked for DME of new capabilities within OCIO and HUD's program offices, such as Federal Housing Administration, Office of Public and Indian Housing, and Office of the Chief Financial Officer initiatives.

HUD did receive some flexibility with its IT funds that it had requested. First, HUD was permitted to transfer up to \$500,000 per project for small-scale IT development from program office salary and expense funds with an overall limitation of \$5 million in the FY. This will permit program offices to provide some of the cost of small IT projects that they need developed, but which OCIO had not yet planned for from the IT Fund. Second, a requirement to receive approval before spending more than 10 percent of DME funds was lifted, although HUD will still need to provide quarterly reports on this project.

However, one requested flexibility was denied. HUD had requested in multiple previous fiscal years and in FY 2024 to include end-user and wireless devices in its Working Capital Fund so that these costs can be billed back to the program offices. This request was not included in the FY 2024 appropriations language.


Conclusion

According to the FY 2024 IG FISMA metrics guidance, an agency’s InfoSec program is effective at maturity level 4, managed and measurable. HUD’s InfoSec program was determined to be not effective, although HUD made significant progress from previous years. We assessed HUD at maturity level 3, consistently implemented, based on our evaluation of the 20 core metrics and 17 FY 2024 supplemental metrics within the 9 domains from the FY 2024 IG FISMA reporting guidance. Table 3 summarizes the assessed ratings of each domain and metric.

Table 3. FISMA rating summary

NIST CSF function	FISMA domain	Ad hoc	Defined	Consistently implemented	Managed and measurable	Domain maturity
Identify	Risk management	0	3	3	1	Consistently implemented
	Supply chain risk management	1	1	0	0	Defined
Protect	Configuration management	0	1	4	0	Consistently implemented
	Identity and access management	0	3	1	0	Defined
	Data protection and privacy	0	0	1	3	Managed and measurable
	Security training	0	0	0	3	Managed and measurable
Detect	Information security continuous monitoring	0	0	3	0	Consistently implemented
Respond	Incident response	0	0	1	4	Managed and measurable
Recover	Contingency planning	0	0	1	3	Managed and measurable
Overall		1	8	14	14	Consistently implemented

HUD continued to take positive steps to improve its IT security posture, increasing maturity in 22 of the 37 metrics, and maintained the same maturity level for the remaining 15 metrics. These changes in maturity were much improved compared to HUD’s progress in prior fiscal years. HUD improved in maturity level from the FY 2023 FISMA evaluation, in which HUD was assessed as maturity level 2, defined, to maturity level 3, consistently implemented, in FY 2024. HUD’s maturity in the FY 2024



supplemental metrics was higher than the maturity of the core metrics, which was also noted in the FY 2023 evaluation.

HUD improved in three of five functions, reaching the managed and measurable level of maturity for the respond and recover functions and the consistently implemented level for the protect function. HUD's achievement of the managed and measurable maturity level in the respond and recover functions represented an effective level of maturity for the first time. HUD remained at the same level of maturity for two of five functions with the identify function maintaining the defined level of maturity and the detect function maintaining the consistently implemented level of maturity.

However, HUD continued to show limitations in establishing its SCRM program and managing and resourcing its ICAM program. HUD OCIO should continue addressing open recommendations from previous FISMA evaluations; develop, modernize, and enhance its legacy systems; strategically utilize its resources, including staff and funding; and deploy technology necessary to implement critical security controls.

This report contains five recommendations to assist HUD in increasing its maturity level within the metrics, domains, functions, and overall InfoSec program. Additionally, as HUD's OCIO and Office of Administration continue to address the remaining open FISMA recommendations, HUD will make progress toward improving the maturity of its InfoSec program.

Recommendations

1. HUD OCIO should:
 - a. resolve the conflicts between its Inventory of Automated Systems (IAS) policy and web applications policy to clarify if web applications will be inventoried in IAS, the web application SharePoint site, or both; and
 - b. implement the chosen resolution to this conflict to develop a consistent inventory of web applications (IG FISMA metric 1).
2. HUD OCIO should implement an automated governance, risk, and compliance tool to manage risk from all sources across the three tiers of the organization in a timely manner. This recommendation updates FY 2021 FISMA recommendation number 5 (IG FISMA metrics 5, 9, and 10).
3. HUD OCIO should employ automation to maintain a timely and accurate view of security configuration information for all systems connected to its network (IG FISMA metric 20).
4. HUD OCIO should demonstrate that it can implement its defined security responses if a baseline configuration is changed without authorization. This can be shown either by a response to a real incident if one happens or through a testing exercise if there are no applicable incidents (IG FISMA metric 23).
5. HUD OCIO should review its security training program and determine whether it should provide general cybersecurity awareness training to external users of its systems and data (IG FISMA metric 44).

Appendixes

APPENDIX A – AGENCY COMMENTS AND OIG’S RESPONSE

Agency Comments



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

CHIEF INFORMATION OFFICER

October 7, 2024

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

FROM: Paul Soot, Business Change & Integration Officer

SUBJECT: HUD comments to Draft FY24 FISMA Evaluation (2024-OE-0002)

This memorandum is in response to the Office of the Inspector General (OIG) draft report *Draft FY24 FISMA Evaluation (2024-OE-0002)*. The Office of the Chief Information Officer (OCIO) has carefully reviewed the Draft Report and accept the five recommendations. We have also attached our technical comments.

If you have questions or require additional information, please contact Yumiko Ito, Acting Deputy to Business Change Integration Officer, at (202)-402-2990 (yumiko.ito@hud.gov), or Ahmed J. Bouaichi, Special Advisor, at (202) 431-7675 (ahmed.j.bouaichi@hud.gov)

Enclosures:
Technical Comments



OIG Response

HUD had no formal comments to the draft report and concurred with the five new recommendations in this report. HUD provided technical comments related to the number of recommendations closed during FY 2024. Overall, HUD closed 34 recommendations in FY 2024 with 27 of those recommendations coming from previous FISMA reports. We encourage HUD to continue its progress made in closing recommendations in FY 2024. Each FISMA recommendation is associated with an IG FISMA metric. This association should enable HUD to better prioritize maturing each component of its InfoSec program.

APPENDIX B – SCOPE, METHODOLOGY, AND LIMITATIONS

Scope

As part of the Federal Information Security Modernization Act of 2014 (FISMA) reporting, each agency Inspector General (IG) or an independent external auditor is required to conduct an annual independent evaluation to determine the effectiveness of the information security (InfoSec) program and practices of its respective agency.¹⁶ The scope of our review was department-wide, resulted in conclusions and recommendations made at the Department level, and covered the period October 1, 2023, to September 30, 2024.¹⁷

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.¹⁸ 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.

Fieldwork was based on the FY 2023-2024 IG FISMA Reporting Metrics¹⁹ and associated CyberScope reporting questions. We assessed the core metrics and the FY 2024 supplemental metrics for a sample of information systems from the U.S. Department of Housing and Urban Development's (HUD's) Inventory of Automated Systems (IAS). We then reviewed HUD's progress toward addressing prior recommendations. This supplemental review was designed to address key deficiencies found during prior FISMA evaluations. Our approach included the following techniques:

- inquiries with management and systems personnel.
- inspection of documentation related to the implementation of FISMA.
- inspection of reports (for example, recent Office of IG (OIG) evaluation reports) related to this evaluation.
- data calls to program offices and system points of contact to gather accurate security program data.
- queries of HUD's Cybersecurity Assessment and Management system to obtain system artifacts.
- queries of HUD's intranet web pages and other accessible sites to collect documentation that was used for verifying information.
- virtual interviews and demonstrations to gain an understanding of information security, privacy, data protection programs and practices, and system operations.
- assessing the implementation and performance of security controls from the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5; and
- security testing to verify the implementation of technical controls.

¹⁶ [Public Law No. 113-283, Federal Information Security Modernization Act of 2014 \(Dec. 2014\)](#)

¹⁷ This narrative report is based on our CyberScope report in Appendix F, which was issued July 24, 2024.

¹⁸ [Quality Standards for Inspection and Evaluation \(ignet.gov\)](#)

¹⁹ [Final FY 2023 - 2024 IG FISMA Reporting Metrics v1.1 \(cisa.gov\)](#)

We evaluated the following organization levels to accomplish our objectives:

Department level – During this step, we gained an understanding of the FISMA-related policies and guidance that HUD Office of the Chief Information Officer (OCIO) established for HUD. We compared HUD’s policies, procedures, and practices to applicable Federal laws and criteria, such as NIST guidance, to determine overall program soundness, effectiveness, and compliance with FISMA.

Program office and system level – We assessed and gained an understanding of the implementation of HUD’s cybersecurity policies and procedures across HUD. Our objective was to obtain this understanding in terms of “program perspective” and “field perspective.” We conducted virtual interviews and demonstrations with program offices in our sample system list. We evaluated the implementation of policies and procedures using the core metrics and FY 2024 supplemental metrics across six program office systems, which are listed in table 4 below.

(b)(5)
(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Reporting

We compiled the information necessary to address the specific reporting requirements outlined in OMB M-24-04, FY 2024 Guidance on Federal Information Security and Privacy Management Requirements.²⁰ Responses to specific IG FISMA reporting metrics were submitted through the DHS web-accessible CyberScope application and in appendix F of this report.

Penetration Testing

Finally, we conducted penetration testing in accordance with FISMA guidance on the selected sample systems' infrastructure and web applications, as applicable. The general framework used by testers included preengagement activities, reconnaissance, scanning, vulnerability analysis, and exploitation. The results of this test will be reported under separate cover.

Limitations

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

²⁰ [OMB M-24-04, FY 2024 Guidance on Federal Information Security and Privacy Management Requirements](#)

APPENDIX C – SUMMARY OF PRIOR FISMA RECOMMENDATIONS

HUD OIG has issued 186 recommendations in our prior annual FISMA evaluation reports since FY 2015. All recommendations from the FY 2015, 2016, and 2017 reports have been closed. Of the 186 recommendations, 56 were still open as of September 30, 2024. This appendix describes the status of the FISMA recommendations in detail. Table 5 shows the distribution of the 56 open recommendations by domain and by the FY in which the recommendation was issued. Figure 5 shows the distribution of open recommendations by the FY in which the recommendation was issued.

Table 5. FISMA evaluation open recommendations by domain (FY 2015-2023)

Domain	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	FY 2023	Domain total
Risk management	(b)(5)						
Supply chain risk management ²¹							
Configuration management							
Identity and access management							
Data protection and privacy							
Security training							
InfoSec continuous monitoring							
Incident response							
Contingency planning							
Fiscal year total	3	3	9	17	4	20	56

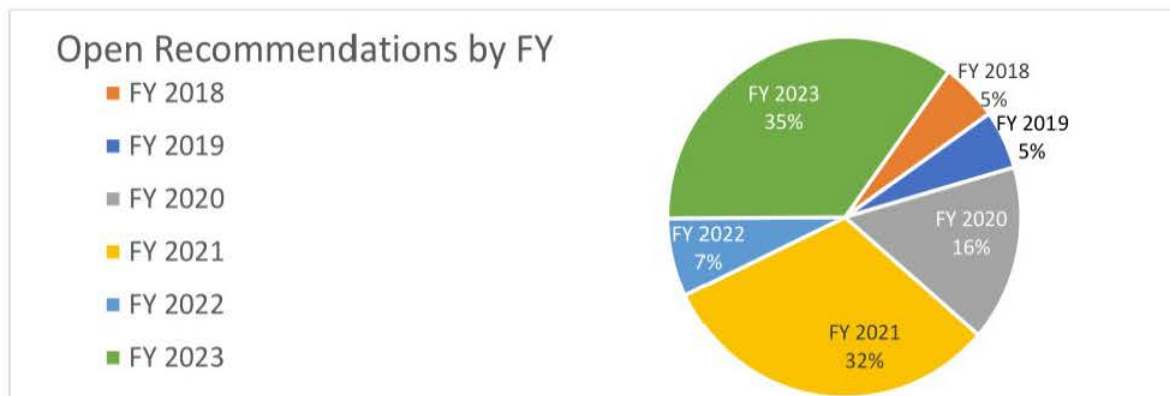


Figure 5. FISMA evaluation open recommendations by FY

²¹ Supply chain risk management was first created as a domain in FY 2021.

HUD made progress in closing recommendations in FY 2024. Overall, 70 percent of our FISMA recommendations have been closed since FY 2015. In particular, the number of recommendations that have remained open for longer than 5 years has decreased from a peak of 18 (in FYs 2019 and 2020) to 2, which demonstrates that HUD has been working on closing its older recommendations.

Finally, table 6 shows HUD’s progress in closing recommendations. In FY 2024, HUD closed 34 recommendations, with 27 of those being FISMA recommendations, which represented 32 percent of the open FISMA recommendations. As HUD’s OCIO and Office of Administration address the remaining open recommendations, HUD will make progress toward improving the maturity of its InfoSec program.

Table 6. FISMA evaluation recommendation closure status

Fiscal year	Total number of recommendations	Number of open recommendations	Number of closed recommendations	Recommendations closed in FY 2024
2015	20	All recommendations (20) closed as of FY 2024		1
2016	14	All recommendations (14) closed as of FY 2022		
2017	19	All recommendations (19) closed as of FY 2024		1
2018	30	3	27	5
2019	26	3	23	6
2020	26	9	17	5
2021	23	17	6	5
2022	5	4	1	1
2023	23	20	3	3
FY totals	186	56	130	27

APPENDIX D – OPPORTUNITIES FOR IMPROVEMENT

We note suggested OFIs below. These issues will not be tracked as formal recommendations but are noted here as general suggestions to improve the effectiveness of HUD's InfoSec program implementation. OFIs are presented at both the enterprisewide and system level. System-specific OFIs were developed based on our evaluation of selected security controls for a sample of HUD program offices.

We have also included the steps that HUD would need to take to achieve level 5—optimized—as OFIs. HUD should consider prioritizing its resources and efforts to achieve level 4—managed and measurable—in metrics first before attempting to increase a metric's maturity to level 5. Both level 4 and level 5 are considered effective levels of maturity. Therefore, we suggest that HUD achieve an effective level of maturity in other metrics before prioritizing improving metrics that are already effective.

Enterprise

Risk Management

1. HUD OCIO should continue to ensure that the Inventory of Automated Systems is updated to include cloud systems (IG FISMA metric 1). This OFI was also reported in FY 2023.
2. HUD OCIO should employ automation to track hardware assets throughout their life cycle with limited manual methods (IG FISMA metric 2). This OFI is written to achieve the optimized level for this metric.
3. HUD OCIO should regularly update its hardware inventory as part of its enterprise architecture current and future states (IG FISMA metric 2). This OFI is written to achieve the optimized level for this metric.
4. HUD OCIO should investigate and resolve the reasons why its CDM dashboard is reporting (b)(7)(C) percent asset coverage, because this could represent unauthorized assets on its network (IG FISMA metric 3).
5. HUD OCIO should address mobile applications as part of its software development life cycle, including a process for inventorying them (IG FISMA metric 6).
6. HUD OCIO should include enterprise architecture review of all IT-related contracts, including those under the \$250,000 threshold (IG FISMA metric 6).

Supply Chain Risk Management

7. HUD OCIO should implement its newly defined supply chain risk management (SCRM) policies and procedures, including completing the transition from NIST SP 800-53, Rev. 4 to Rev. 5 (IG FISMA metric 14).
8. HUD OCIO should ensure that the questionnaire that it intends to implement as part of its SCRM procedures provides sufficient assurance that systems and services provided by external partners meet applicable FISMA, NIST, OMB, and HUD guidance (IG FISMA metric 14).

9. HUD OCIO should ensure that it maintains visibility into its upstream suppliers and can monitor changes in those suppliers (IG FISMA metric 14).

Configuration Management

10. HUD should define roles and responsibilities for configuration management, including for authorizing officials and system owners. In addition, HUD should finalize the roles and responsibilities listed for “users” in the Configuration Management Process Guide, which has 17 instances of “TBD” listed in the document (IG FISMA metric 17).
11. HUD OCIO should ensure that configuration management plans and configuration management templates include roles and responsibilities for authorizing officials (IG FISMA metric 17).
12. HUD OCIO should provide further information about its configuration management accountability process so that it can be evaluated for increased maturity (IG FISMA metric 17).
13. HUD OCIO should continue to review configuration management plans across the organization to ensure that they comply with the enterprise configuration management plan (IG FISMA metric 18).
14. HUD OCIO should finish integrating its configuration management lessons learned plan with its Project Planning and Management program (IG FISMA metrics 18, 20, and 23).
15. HUD should continue to remove legacy hardware and software that are no longer in use, including removing tailored hardening guides that are not needed (IG FISMA metric 20).
16. HUD should provide the results of its scans in future FISMA evaluations to OIG so that OIG can independently verify that the scans are taking place and that detected issues are being resolved in a timely manner (IG FISMA metrics 20 and 21).
17. HUD OCIO should document the requirement that scans be performed every 72 hours if it intends to execute the scans at that frequency (IG FISMA metrics 20 and 21). This OFI was also reported in FY 2023.
18. HUD OCIO should remove the exemption that allows web applications to be scanned only once per year (IG FISMA metrics 20 and 21).

Identity, Credential, and Access Management

19. HUD OCHCO should implement a tool that automates the documentation and tracking of risk designation and screening information (IG FISMA metric 28)
20. HUD OCIO should implement procedures to ensure that quarterly privileged user account reviews are consistently performed and documented in accordance with HUD’s defined policies (derived from OIG FISMA metric 32).

Data Protection and Privacy

21. HUD OCIO, the HUD Privacy Office, and the HUD Records Office should finish updating its media sanitization procedures and form(s) to account for its various disposal streams.
22. HUD OCIO should ensure that its security controls for protecting PII and other agency sensitive data throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.
23. HUD OCIO should develop a strategy and capability to continuously run risk-based device posture assessments (e.g., using EDR tools) to proactively identify vulnerabilities and key risks as part of its data exfiltration defenses.
24. HUD OCIO and the HUD Privacy Office should fully coordinate and integrate its Data Breach Response Plan with the incident response, risk management, continuous monitoring, continuity of operations and other mission/business areas.
25. HUD OCIO should fully document and integrate its data exfiltration and network defenses into the ISCM and incident response programs to provide near real-time monitoring of data entering and exiting the network.
26. HUD OCIO and the HUD Privacy Office should institutionalize a process of continuous improvement and develop the capability to maintain ongoing awareness of threats and vulnerabilities that may pose privacy risks and provide timely training on those identified risks.
27. The HUD Privacy Office should continuously strategize and update its privacy training practices and technologies as needed to adapt to changes in the privacy and information technology landscape.

(b)(5)

(b)(5)

APPENDIX E – LIST OF ABBREVIATIONS

Acronym	Definition
BIA	business impact analysis
CDM	continuous diagnostics and mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CSAM	Cybersecurity Assessment and Management
CSF	Cybersecurity Framework
DHS	U.S. Department of Homeland Security
DME	development, modernization, and enhancement
DRGR	Disaster Recovery and Grants Reporting system
EDR	endpoint detection and response
EO	executive order
EWBIA	enterprisewide BIA
FHA	Federal Housing Administration
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
Ginnie Mae	Government National Mortgage Association
GMEPS	Ginnie Mae Enterprise Portal System
GRC	governance, risk, and compliance
GSS	general support system
HUD	U.S. Department of Housing and Urban Development
HVA	high-value asset
IAS	Inventory of Automated Systems
ICAM	identity, credential, and access management
IG	Inspector General

InfoSec	information security
ISCM	information security continuous monitoring
ISVI	Information systems vulnerability information
IT	information technology
LOCCS	Line of Credit Control System
M	memorandum
MEF	mission-essential function
MFA	multifactor authentication
NIST	National Institute of Standards and Technology
NSPIRE	National Standards for the Physical Inspection of Real Estate
O&M	operations and maintenance
OA	ongoing authorization
OCIO	Office of the Chief Information Officer
OFI	opportunity for improvement
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
POA&M	plan of action and milestones
RFS	Reporting and Feedback System
SCRM	supply chain risk management
SIEM	security information and event management
SOC	Security Operations Center
SP	special publication
TIC	Trusted Internet Connection
TMF	Technology Modernization Fund
ZTA	zero-trust architecture



APPENDIX F – FY 2024 HUD OIG CYBERSCOPE SUBMISSION

The inserted document below contains the IG responses to the FY 2024 IG FISMA metrics, established by OMB. OMB issued M-24-04, FY 2024 Guidance on Federal Information Security and Privacy Management Requirements, on December 4, 2023. The memorandum details required FISMA reporting instructions. The document below was submitted to DHS' CyberScope portal on July 24, 2024.

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



APPENDIX H – 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

Blake Hayes, Senior IT Evaluator

Craig Wood, Senior IT Evaluator

Mackenzie Averill, Senior IT Evaluator