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

HUD Fiscal Year 2023 Federal Information Security Modernization Act of 2014 Evaluation Report

Washington, DC | 2023-OE-0001

January 29, 2024

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

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: January 29, 2024

To: Marcia L. Fudge
Secretary, S

From: Rae Oliver Davis
Inspector General, G

Rae Oliver Davis

Subject: Fiscal Year 2023 Federal Information Security Modernization Act of 2014 Evaluation Report and Inspector General Metric Responses

We have completed our fiscal year (FY) 2023 Federal Information Security Modernization Act of 2014 (FISMA) evaluation. Our final report (FY 2023 FISMA Evaluation Report, Number 2023-OE-0001) and our responses to the annual Office of Inspector General (OIG) 2023 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 2023 OMB instructed IG's to focus the evaluation on 20 core and 20 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 2023 overall FISMA maturity was assessed at level 2, the "defined" maturity level, which remained the same as its FY 2022 maturity level. This outcome is despite HUD's increasing maturity in 10 of 40 metrics, remaining at the same maturity level for 25 metrics, and dropping in maturity in 5 metrics, which was statistically consistent with prior fiscal years.

Our report highlights the strengths and weaknesses in each of the nine domains and provides recommendations to assist in addressing those weaknesses. The report also recognizes HUD's initiatives to improve the HUD InfoSec program. We encourage HUD to continue the improvements, address our recommendations, and establish priorities to achieve an effective InfoSec program. The attached narrative report provides an executive summary and detailed results for each domain. We provide 23 new recommendations and 66 opportunities for improvement, with only the recommendations being formally tracked by our office. The report associates each FY 2023 HUD OIG recommendation to an IG FISMA metric. This association should enable HUD to better prioritize maturing each component of its IS 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.

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 risk management, data protection and privacy, information security continuous monitoring, and incident response 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.

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 2023 FISMA Evaluation Report (2023-OE-0001)

Cc: Adrianne Todman, Deputy Secretary
Julienne Joseph, Chief of Staff
Damon Smith, General Counsel
Beth Niblock, Chief Information Officer
Elizabeth de León Bhargava, Assistant Secretary of Administration
Vinay Singh, Chief Financial Officer
Sairah Ijaz, Principal Deputy Chief Information Officer
Gregg Kendrick, Chief Information Security Officer
Russell Ramos, Deputy Chief Information Security Officer
David Peters, Chief Technology Officer
Juan Sargeant, Assistant Chief Information Officer for Infrastructure and Operations
Paul Scott, Business Change and Integration Officer
Gina Metrakas, Chief Operating Officer
Florence Lynk, Office of Public Affairs
Julia Gordon, Federal Housing Administration
Richard Monocchio, Principal Deputy Assistant Secretary for Public and Indian Housing
Solomon Greene, Principal Deputy Assistant Secretary for Policy Development and Research
Michele Perez, Field Policy and Management

This page intentionally left blank

Executive Summary

FISCAL YEAR 2023 FISMA EVALUATION REPORT | 2023-OE-0001

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) fiscal year (FY) 2023 IG FISMA Metrics consisted of nine domains aligned with the five functional areas from the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF). A total of 40 metrics were evaluated in FY 2023, which included 20 core metrics that are assessed annually and 20 FY 2023 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 level 5 representing optimized. OMB and the Office of Inspector General's (OIG) FISMA metric guidance state that an agency InfoSec program is effective at maturity level 4, which is managed and measurable.

Findings

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, HUD's InfoSec program was at level 2, "defined," which is a level considered not effective. HUD increased in maturity for 10 metrics, decreased in maturity for 5 metrics, and maintained the same maturity for 25 metrics. Notably, HUD achieved the level 4, "managed and measurable" maturity level for the first time in 2 metrics. A summary of HUD's maturity level distribution is provided in figure 1.

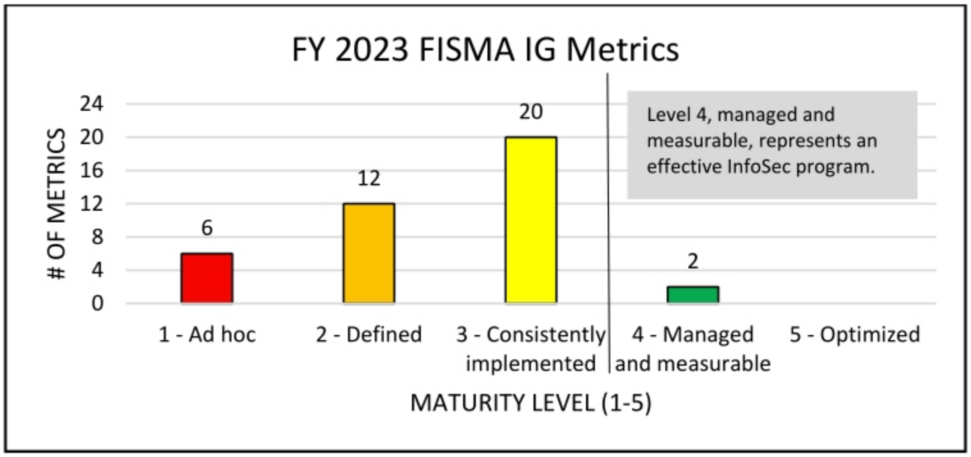


Figure 1. HUD maturity level distribution

HUD's InfoSec program averaged a score of 2.60 for the 20 core metrics and a 2.86 for the FY 2023 supplemental metrics,[1] both of which are at the "defined" maturity level and are considered not effective. Although HUD improved overall, four of the five metrics in which HUD dropped in maturity were core metrics. HUD made commendable progress on increasing maturity on 10 metrics and should continue to focus on prioritizing maturity in the 20 core metrics and key cyber executive orders and requirements outlined in the introduction 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 (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 risk management, data protection and privacy, information security continuous monitoring, and incident response programs.

HUD's risk management program supports a structured but flexible process to provide senior leaders with the necessary information to make efficient, cost-effective, risk management decisions about the systems supporting their missions and business functions; and incorporates security and privacy into the system development life cycle. By improving its risk management program, HUD would be able to better understand, prioritize, and address the most critical IT risks by IT system and program. In addition, HUD would be able to prevent malicious or risky software from running on HUD's systems by blocking that software that wasn't already known and approved. HUD continued to show progress but still did not have consistent or complete hardware and software inventories.

In support of its mission, HUD operates many large-scale programs designed to serve the public. The information systems supporting these programs maintained at least a billion records containing PII and daily facilitated thousands of transactions with business partners and private individuals. Although HUD's enterprisewide privacy program made improvements in FY 2023, it needs to continue to make significant progress in allocating adequate resources to the Privacy Office, improving its removable media and sanitization processes, and implementing tools and solutions to strengthen its data exfiltration prevention and network defenses maturity.

The continuous monitoring program requires maintaining an ongoing awareness of InfoSec, vulnerabilities, and threats to support organization risk management decisions. With an effective ISCM program, HUD would be able to implement all required automated tools and strategies to report on agency data with the goal of managing risk and self-identify key areas within FISMA for improvement. While HUD had made progress in its ISCM program, it needs to continue to enroll and authorize its systems and collect and analyze data to further mature the program.

HUD's incident response capability could rapidly detect incidents, minimize loss and destruction of data, mitigate any weaknesses that are exploited, and restore IT services in a timely manner based on business priority. We continued to see improvement in the incident response capability. However, HUD needs to

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

comply with OMB requirements[2] for standardized and comprehensive logging, which is essential for detecting, investigating, and remediating cyber threats.

Significant challenges continue 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.

HUD was still establishing its SCRM program in FY 2023, including developing a strategy, policies, and procedures. 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. A mature program would increase HUD's ability to discover and address vulnerabilities, for example, with a third-party vendor's software.

HUD's configuration management program comprises a collection of activities focused on establishing and maintaining the integrity of IT systems, through control processes for initializing, changing, and monitoring configurations, throughout the system development lifecycle. Improvements in this domain would allow HUD to complete consistent configuration scans, resulting in the ability to remain in compliance with system baseline requirements and remediate critical vulnerabilities that, if left unpatched, could result in a breach.

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 moves towards more secure methods of access and authorization, HUD continued to lack multifactor authentication (MFA) for all but two of its systems. In compliance with provisions of EO 14028 and related implementing guidance within OMB M-22-09, agencies are required to progress toward a zero-trust architecture (ZTA) 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.

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

HUD continued to make significant progress in addressing our prior years' recommendations. During FY 2023, HUD closed 9 prior FISMA recommendations that improved its risk management, privacy, security training, and contingency planning programs. In this report, we offer 23 new recommendations and offer

[2] OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

additional opportunities for improvement[3] (OFI) for the enterprise and program offices. The recommendations issued in FY 2023 were primarily focused on identified weaknesses within the risk management and ICAM domains, which had declined in metric maturity.

[3] 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.

Table of Contents

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 FISMA the assessment and provide recommendations and opportunities for improvement to help HUD to better prioritize maturity each component of its InfoSec program.

FISMA Overview

The Federal Information Security Management Act of 2002,[4] as amended by FISMA,[5] establishes the following responsibilities for agency heads:

- providing IS 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 IS 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) 2023 CIO metric responses should reflect the implementation of

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

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

cybersecurity-related initiatives, including those in support of Executive Order (EO) 14028, Improving the Nation's Cybersecurity. [6]

IG FISMA METRICS

OMB's Office of the Federal CIO issued the FY 2023-2024 IG FISMA Reporting Metrics on February 10, 2023.[7] 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 can use to report additional information for each domain.

We evaluated the 20 core metrics and the 20 FY 2023 supplemental metrics. We did not evaluate the FY 2024 supplemental metrics, because they were not intended to be assessed this year. HUD OIG does not generally use the nine optional domain summary metrics. In total, 40 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),[8] 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	▪ Risk management ▪ Supply chain risk management
Protect	▪ Configuration management ▪ Identity and access management ▪ Data protection and privacy ▪ Security training
Detect	▪ InfoSec continuous monitoring
Respond	▪ Incident response
Recover	▪ Contingency planning

[6] OMB M-23-03, FY 2023 Guidance on Federal Information Security and Privacy Management Requirements.

[7] FY 2023 - 2024 IG FISMA Reporting Metrics

[8] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1

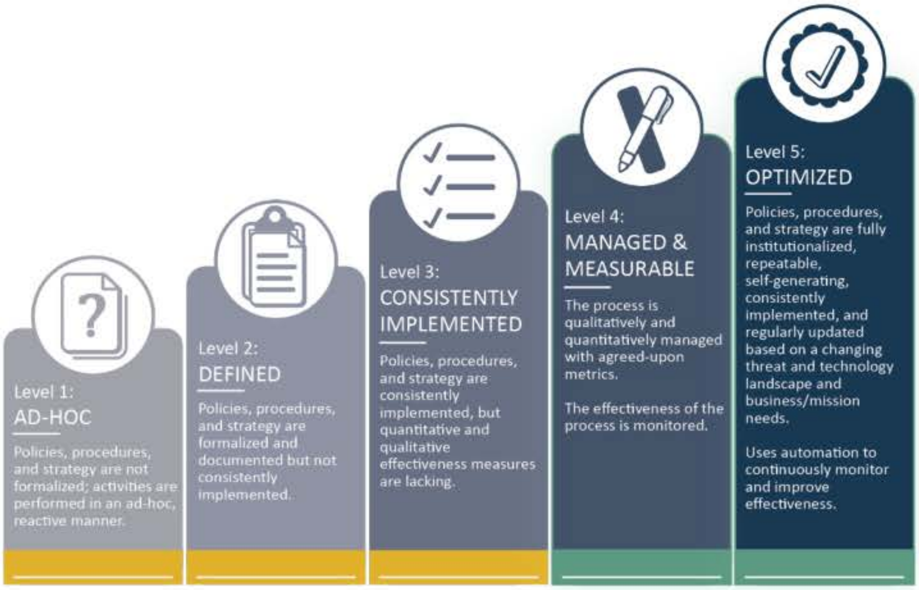
IG FISMA Core Metrics

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 EO 14028.[9] 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, level 4—managed and measurable—represents an effective level of security, as shown below in figure 2.[10] The maturity levels for the five NIST CSF functions together measure the overall InfoSec program effectiveness.



Level 1:
AD-HOC

Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.

Level 2:
DEFINED

Policies, procedures, and strategy are formalized and documented but not consistently implemented.

Level 3:
CONSISTENTLY IMPLEMENTED

Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

Level 4:
MANAGED & MEASURABLE

The process is qualitatively and quantitatively managed with agreed-upon metrics.

The effectiveness of the process is monitored.

Level 5:
OPTIMIZED

Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Uses automation to continuously monitor and improve effectiveness.

Figure 2. IG FISMA maturity model levels

[9] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[10] Security and Privacy Controls for Information Systems and Organizations (nist.gov) 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.

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 2023 FISMA evaluation narrative report. Appendix B describes the scope and methodology used to complete the evaluation.

Results of Review

SUMMARY AND OVERALL MATURITY LEVEL

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, HUD's InfoSec program was evaluated as level 2, "defined," which is considered not effective. HUD's overall InfoSec program scored a 2.60 for the core metrics and a 2.86 for the FY 2023 supplemental metrics. Although HUD had made improvements in metrics across all domains, it had declined in maturity in five metrics, four of which were core metrics. 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.

HUD achieved the consistently implemented maturity level in three of the five functions and was at the defined maturity level for the remaining two functions. HUD continued to demonstrate consistently implemented programs for the detect, respond, and recover functions, including information security continuous monitoring (ISCM), incident response, and contingency planning programs.

However, HUD continued to show limitations in the identify and protect functions, specifically with establishing its supply chain risk management (SCRM) program, executing its configuration management 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 by domain from the metric assessment to discuss in this report. See table 2 for HUD's maturity level in each domain, function, and overall InfoSec program. Please see appendix F for the full CyberScope report for all 40 metrics assessed in FY 2023.

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)	2 – defined
Supply chain risk management	1 – ad hoc		
Configuration management	2 – defined	2 – defined (protect)	
Identity and access management	2 – defined		
Data protection and privacy	3 – consistently implemented		
Security training	3 – consistently implemented		
InfoSec continuous monitoring	3 – consistently implemented	3 – consistently implemented (detect)	
Incident response	3 – consistently implemented	3 – consistently implemented (respond)	
Contingency planning	3 – consistently implemented	3 – consistently implemented (recover)	

RISK MANAGEMENT

The risk management domain is foundational to several other domains for three primary reasons. First, risk management includes identifying IT assets and determining their associated risks. Other domains, such as configuration management, data protection and privacy, ISCM, incident response, and configuration management, need accurate asset inventories to be effective. Second, the risk management domain includes prioritizing and communicating mitigation efforts of identified risks. HUD used plans of action and milestones (POA&M)[11] as its main method of tracking and communicating risks. Identifying and monitoring risks through POA&Ms is the first step in defending the organization from those risks. Finally, the risk management domain involves assigning roles and responsibilities for risk management to appropriate stakeholders and then holding them accountable for their performance. Knowing what role is responsible for each risk management task and ensuring that they are performing those tasks effectively is necessary to ensure the overall risk management program is effective. Overall, HUD regressed in maturity in this domain in FY 2023 as shown in table 3. As HUD focuses on progressing in its risk management practices, it will set a solid foundation for improvement in other domains as well.

Table 3. Risk management core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
1	(b)(5)		
2			
3			
5			
7			
8			
9			
10			

Spotlights on Success

- HUD defined and implemented a requirement for including cloud and other external systems into its system inventory, which provided a more comprehensive view of its IT systems.
- HUD's processes to share cybersecurity risk management information were integrated with its ISCM program.
- HUD has developed performance measures on which it intends to collect data, which, once implemented, would support increased maturity in this domain.

Program Improvement Needs

- HUD had a discrepancy of (b)(5) devices between its list of authorized hardware assets and hardware assets detected on its network.

[11] A POA&M identifies a security weakness and provides a list of tasks to resolve the security weakness, milestones for completing the tasks, and required funding resources.

- HUD had not yet addressed the critical software or critical software platform requirements from EO 14028.
- HUD did not demonstrate that it was allocating resources in a risk-based manner or holding stakeholders accountable for the performance of their risk management duties.

Domain Summary

The first area of the risk management domain assessed HUD's maturity in maintaining inventories of its systems, hardware assets, and software assets, with HUD demonstrating some progress. HUD had improved the coverage of its system inventory to include cloud and other external systems, which had been noted as a weakness in prior evaluations. HUD must ensure that cloud and external systems meet its security requirements, even if the systems are maintained by external partners. Maintaining a list of these types of external systems was the first step to making sure that these security requirements were met. However, this progress did not demonstrate that HUD had consistently implemented its inventory processes. Overall, there were five weaknesses with HUD's inventory processes that we identified this year.

First, HUD still had web application system information that was maintained outside HUD's official system inventory repository, the Inventory of Automated Systems (IAS). OCIO closed a Priority Open Recommendation by promulgating a policy that all web applications had to be approved by OCIO. The policy required all web applications to be documented in IAS. Having system information in multiple repositories contributed to preventing HUD from having a comprehensive list of system information.

Second, HUD did not consistently maintain its records of system interconnections, which was necessary to understand data flows across the organization. Without an accurate and updated list of interconnections, HUD would not be able to determine normal data flows between systems; therefore, it would also be unable to differentiate anomalous data flows from normal data flows.

Third, HUD did not have a consistent list of hardware assets, which it had in previous years. The list of assets detected on HUD's network included (b)(5) devices that were not on the list of assets authorized to be on the network. Unauthorized hardware devices pose a risk to the network, both in the form of potentially malicious actors' being connected to the network and in maintaining comprehensive patch management and flaw remediation for these devices.

Fourth, HUD did not show that it had a comprehensive inventory of software assets and licenses. Without an accurate inventory of software assets and licenses, HUD could not verify that only authorized software was installed on its network. HUD's processes compensated for this risk by requiring OCIO involvement to install software on network devices, but this mitigation would not prevent an insider with elevated privileges from installing unauthorized software. In addition, incomplete software license information could lead to violations of license agreements or wasted resources on unused licenses, as recently reported in the National Aeronautics and Space Administration (NASA) by NASA OIG in January 2023.[12]

Fifth, HUD did not make progress toward two new OMB requirements that took effect in FY 2023. HUD did not show that it was reporting at least 80 percent of its government-furnished equipment through the

[12] Final Report - IG-23-008 - NASA's Software Asset Management (oversight.gov).

DHS Continuous Diagnostics and Mitigation (CDM) program.[13] Additionally, HUD did not address critical software in its software asset inventory policies, procedures, or implementation. EO 14028 mandated that agencies inventory their critical software and the platforms that run critical software, which was a new requirement for OIGs to assess in FY 2023.

The next area of the risk management domain considered HUD's maturity in assessing, tracking, and communicating risk to the appropriate stakeholders at all levels of the organization, including the individual system level, program office level, and enterprisewide level. HUD maintained its maturity in this area, with both slight improvements and regressions.

First, at the system-level, HUD continued to consistently conduct annual risk assessments, which was critical to maintaining awareness of the risks that the systems faced. Similar to how HUD as an organization cannot defend against risks that it has not identified, individual systems cannot protect against risks that have not been identified at the system level. Four of the eight sample systems had updated risk assessments, and one additional sample system had been identified and contacted by OCIO to perform its assessment. However, (b)(5)
(b)(5)

HUD also continued to consistently document POA&Ms at the system level in its Cybersecurity Assessment and Management system (CSAM). In addition, HUD's authorizing officials were consistently involved in the risk-based decision process, which had not been the case in previous evaluations.

Next, at the program office level, HUD consistently maintained risk registers. When risks were identified in one program office that impacted the mission or function of another program office, those risks were transferred from the identifying program office to the program office that could better track and address the risks. However, HUD's program offices still needed to show that its risk responses were being monitored over time. A risk response that was acceptable when it was first assessed may no longer be tolerable over time due to changes in the risk or changes in HUD's risk appetite. In either case, the risk response would need to be reevaluated. HUD has an open recommendation to address this finding.

Program offices also had POA&Ms that did not follow the approved template to document risk-based decisions in CSAM or ensure that the risks were communicated to OCIO. This result is an example in which communication between program offices is key to ensuring that all stakeholders are consulted and informed about risks in their respective areas.

Finally, at the enterprise level, there were two main weaknesses for HUD to address to improve its maturity. First, HUD's risk information was not normalized across different program offices. HUD could not demonstrate that it effectively converted risk ratings from multiple program offices into an enterprise risk rating, which was required to normalize risk information across program offices. Without normalized risk information, the enterprise risk management (ERM) program would not be able to effectively prioritize risks that were rated on different scales. Further, without effective prioritization, HUD would

[13] As required by OMB M-23-03, FY 2023 Guidance on Federal Information Security and Privacy Management Requirements.

then be unable to effectively allocate resources to its most important risks. HUD has an open recommendation to address this issue.

The second weakness at the enterprise level was related to how HUD communicated risk information to the appropriate stakeholders. HUD primarily planned to use dashboards to communicate risk information to stakeholders, but these dashboards were only used in the second half of FY 2023 after HUD onboarded contractor support to implement the dashboards. Without timely and accurate risk information from the dashboards, HUD stakeholders could not effectively prioritize risks to ensure that resources were prioritized to address the most significant threats. HUD has an open recommendation to address this issue.

The final area of the risk management domain assessed HUD's maturity in implementing, resourcing, and monitoring the roles and responsibilities of its risk management personnel. HUD's risk management personnel were consistently implementing their roles and responsibilities. However, HUD should consolidate and formally document these roles and responsibilities so that a person in a particular role could see his or her responsibilities in one consolidated location.

Further, HUD did not show that it allocated resources in a risk-based manner to ensure that cybersecurity risk management activities were effectively supported. HUD provided evidence of IT-related hiring actions that OCIO personnel believed would assist in implementing cybersecurity risk management activities. However, this evidence was not sufficient because it did not demonstrate OCIO taking a risk-based approach to prioritizing hiring actions. Further, risk-based allocation of resources includes all types of resources, not just personnel, and we received no evidence that other forms of resources, such as funding or technologies, were being allocated in a risk-based way.

Finally, HUD did not show that it was effectively monitoring the performance of cybersecurity risk management stakeholders in their roles and responsibilities. HUD used POA&Ms as evidence of stakeholder accountability. However, POA&Ms are evidence of the tracking, monitoring, and eventual remediation of a specific security or system vulnerability, not that stakeholders are effectively performing their roles and responsibilities. For example, a system might have more POA&Ms because it is a legacy system, not because the stakeholders responsible for that system are not performing their roles to update the system effectively. Similarly, a system with stakeholders who ignore vulnerabilities and do not document them in POA&Ms might appear to have a lower number of outstanding POA&Ms, but they would not be effectively performing their roles. Finally, using POA&Ms as a stakeholder accountability process also does not cover cybersecurity risk management stakeholders above the system level, such as the personnel responsible for integrating program office risk management information with the ERM program, since POA&Ms were not used to track their performance effectiveness.

We offer 10 recommendations and 25 OFIs for HUD to increase maturity in this domain. In addition, HUD has 12 open risk management domain recommendations from previous FISMA evaluation reports, as noted in appendix C.

SUPPLY CHAIN RISK MANAGEMENT

HUD relies on a diverse range of IT products and services to accomplish its mission, making the management of supply chain risks essential for maintaining effective IT security. SCRM is an organized process for managing exposure to IT security risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. The acquisition of IT resources involves complex, globally distributed supply chains with multiple layers of outsourcing, making it challenging to gain visibility, understanding, and control of supply chain cybersecurity risks. Compromises in the supply chain may lead to cascading effects across various FISMA domain functions; therefore, SCRM is a critical aspect of HUD's overall IT security. For instance, an undiscovered vulnerability with a third-party vendor's software could lead to a breach in identity and access controls, bypass of data protection controls, and activation of incident response and contingency plans. Highly publicized supply chain compromises in recent years highlight the broad impacts possible and underscore the need for an effective SCRM program. While HUD had advanced in this area, it remained in the early stages of developing its enterprise SCRM program.

Table 4. Supply chain risk management core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
12	(b)(5)		
13			
14			

Spotlights on Success

- HUD defined and communicated an enterprisewide SCRM strategy for managing the IT supply chain risks.
- HUD updated its information system contingency plan procedures, IT security control catalog, and ISCM procedures, to include SCRM considerations.

Program Improvement Needs

- HUD had not developed or implemented SCRM program policies and procedures.
- Program offices had limited awareness of HUD's SCRM strategy.
- HUD did not have SCRM tools or methods to confirm that contractors were meeting their contractual SCRM obligations.

Domain Summary

HUD remained at the ad hoc maturity level for SCRM; however, it had made progress in several areas. HUD created an SCRM strategy, which helps to set the roles and expectations for implementing a coordinated enterprise program. HUD also established an SCRM executive subcommittee under its Enterprise Risk Management Council to provide SCRM program oversight. This subcommittee included members from each program office. Officials interviewed from HUD's OCIO and Office of the Chief Procurement Officer (OCPO) indicated that necessary resources were available to implement the strategy, including a contract to assist with developing SCRM policies and procedures and implementing an enterprisewide SCRM program. Within its IT acquisition processes, HUD developed contract language for inclusion in future IT contracts mandating vendor compliance with Federal SCRM guidance and designed a questionnaire that could be used in the future to assess the supply chain risks associated with prospective vendors during IT procurements. HUD had also updated its information system contingency plan procedures, IT security control catalog, and ISCM procedures to include SCRM considerations.

Despite this progress, HUD remained at the initial stages of developing an SCRM program and had not yet defined comprehensive SCRM policies and procedures to ensure all necessary elements of SCRM are addressed. HUD needs to develop procedures for identifying and prioritizing its externally provided systems, system components, and services and for maintaining awareness of the suppliers used by external providers. HUD also did not have tools or methods to confirm that contractors met their contractual SCRM obligations. Additionally, although OCIO made efforts to communicate its SCRM strategy, program office officials we interviewed as part of our sample system testing had limited awareness of the SCRM strategy. Without defined guidance and standards for implementing an SCRM program, HUD remains at an elevated risk for supply chain related cybersecurity incidents.

We did not offer any new recommendations but offer three OFIs for HUD to increase its maturity in this domain. In addition, HUD has three open SCRM domain recommendations from previous FISMA evaluation reports, as noted in appendix C.

CONFIGURATION MANAGEMENT

HUD's configuration management program focuses on "establishing and maintaining the integrity of its systems through controls of the processes for initializing, changing, and monitoring" configurations throughout a system's life cycle.[14] HUD had improved its configuration management program by collecting and reporting on performance measures for its vulnerability disclosure policy (VDP) program and by consistently showing that it had baseline system configurations. However, HUD did not show that it consistently performed scans to ensure that systems remained in compliance with the baseline or that systems were patched in a timely manner. Specifically, (b)(5) critical vulnerabilities were detected on multiple scans over 14 months, which showed that they had not been timely remediated within HUD's defined timeline of 15 days. Finally, HUD had not updated its trusted internet connection (TIC) program from TIC 2.0 to TIC 3.0, an OMB requirement by the end of FY 2020. Overall, HUD showed progress in its maturity in this domain, as shown below in table 5, by increasing maturity in two metrics. However, HUD still needs to improve in its scanning and TIC programs to achieve the next maturity level for this domain.

Table 5. Configuration management core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
19	(b)(5)		
20			
21			
22			
24			

Spotlights on Success

- HUD demonstrated that it consistently had baseline configurations of its systems, which it had not done in prior years.
- HUD's VDP program collected and reported on performance measures, which led to one of HUD's first two metrics' being rated at the managed and measurable level. HUD had not achieved a managed and measurable level for any metric previously.
- HUD quickly responded to an identified version issue with its publicly posted VDP and resolved it, demonstrating that it is effectively monitoring the VDP program.

Program Improvement Needs

- HUD did not show that scans were being consistently performed, in part due to its lack of a consistent hardware and software inventory.
- HUD had (b)(5) critical vulnerabilities that appeared on multiple scans over 14 months, indicating that critical vulnerabilities were not being patched in a timely manner.

[14] NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems

- HUD had not updated its TIC policies and procedures from TIC 2.0 to TIC 3.0, which was required by September 12, 2020.

Domain Summary

The first area of the configuration management domain assessed HUD's system scanning program. A scanning program, at a high level, is a three-step process. First, HUD needed to have a baseline to scan against to know what a compliant system looked like. Second, HUD needed to consistently perform scans of its systems against their baselines to determine whether the systems were compliant with their defined baselines and any approved deviations. Finally, HUD needed to resolve any issues that were identified in the scan results.

HUD showed progress in the first step by demonstrating that it had an enterprise repository of baseline configurations that included workstations, servers, and network devices. In addition, the sample systems we evaluated were consistently monitored under a configuration management tool. Four of the eight sample systems had updated configuration management records in both IAS and CSAM. However, HUD's baseline configuration repository did not show configurations (b)(5) (b)(5) These types of devices also need baselines so that they can be scanned for compliance and have necessary patches applied. Because these devices were left unscanned, they could be a weak point that an attacker could use to pivot to other parts of the HUD network.

HUD did not show improvement in the second step of consistently performing scans for three primary reasons. First, as noted in the risk management domain, HUD's lack of a comprehensive inventory of its systems, hardware assets, and software assets affected its scanning program. For example, multiple operating systems were not included in configuration scans.[15] Operating systems are the foundation on which all other software runs, so maintaining their configuration is crucial and an insecure operating system can allow for privilege escalation or other attacks. The second limitation of HUD's scanning program was the timing of the scans. OCIO personnel stated that scans were performed every 72 hours. Additionally, OCIO personnel provided scan configurations showing that some scans, but not all scans, were scheduled to run on a cycle with no more than 72 hours between scans. OIG requested scan results from throughout the year to verify the implementation of the scanning schedule. However, the provided scan results were dated monthly or less frequently, which did not show that the scans were being performed every 72 hours. Finally, HUD did not have ".audit" files, which are technical files used to verify that configurations were being scanned in accordance with the defined baselines.

The last step of the scanning process is to use the information in the scans to resolve any issues that were detected by the scans. HUD also did not show improvement in this final step. HUD's lack of a comprehensive inventory also affected its ability to patch systems or assets because of its lack of awareness of those systems and assets. However, HUD stated they were in the process of implementing CDM tools to inventory their assets. Implementing these tools will help ensure in the future that patches are applied to inventoried assets across the organization in a timely manner, which HUD did not achieve in FY 2023. We identified (b)(5) critical vulnerabilities in 5 provided scans covering a period of 14 months.

[15] The specific list of operating systems is listed in Appendix D, Opportunity for Improvement #13.

The repeated presence of these critical vulnerabilities indicated that they were not being remediated in accordance with HUD's defined policy that critical vulnerabilities would be patched within 15 days.

HUD has open recommendations to address issues in all three steps of the configuration management scanning process, and OIG is making an additional recommendation in this report.

The other area of the configuration management domain assessed two required programs. The first program was its TIC. HUD did not show progress in this program. HUD was required to update its policies and procedures from the TIC 2.0 program to the TIC 3.0 program by September 12, 2020,[16] but had not done so and was still using the TIC 2.0 program. HUD stated it was considering two use cases under the TIC 3.0 program. For the TIC program, HUD will also need to show that it has defined processes to maintain an accurate inventory of its network connections to achieve the defined level of this metric. The inventory must include details on the service provider, cost, capacity, traffic volume, logical-physical configurations, and topological data for each connection.

The second program assessed within this domain was HUD's VDP, which is a program where members of the public can submit vulnerability reports to HUD. If a person submitting the vulnerability report follows HUD's processes in the VDP, then HUD agrees not to pursue any law enforcement or civil lawsuits against the person submitting the report, such as for unauthorized access to a HUD system. The VDP process allows security researchers who discover a vulnerability to report it to HUD for remediation without fear of prosecution, which removes a negative incentive to avoid reporting the vulnerability to HUD. This reporting of potential vulnerabilities allows HUD to improve the effectiveness of its InfoSec program.

HUD had achieved an effective VDP program, an improvement on the previous year. HUD collected and monitored performance measures on its VDP program and reported them to DHS as required by Binding Operational Directive 20-01. In addition, we identified a discrepancy between HUD's approved VDP and what was publicly posted, but HUD quickly resolved the issue after it was reported. This quick response demonstrated that HUD was effectively monitoring its VDP program.

Even though the VDP program was effective, HUD can continue to improve the program. There are two improvements to the VDP that HUD could choose to implement. First, HUD can actively adapt its VDP program to provide information to stakeholders on a near real-time basis. Second, HUD can consider the use of a bug bounty program as part of its ERM program. If HUD chooses to implement a bug bounty program, it must ensure that the program meets the requirements of OMB M-20-32.[17] Because the VDP program was assessed as effective, these improvements are listed as OFIs instead of recommendations.

We offer 5 recommendations and 17 OFIs for HUD to increase maturity in this domain. In addition, HUD has 12 open configuration management domain recommendations from previous FISMA evaluation reports, as noted in appendix C.

[16] OMB M-19-26, Update to the TIC Initiative

[17] OMB M-20-32, Improving Vulnerability Identification, Management, and Remediation

IDENTITY AND ACCESS MANAGEMENT

ICAM processes are designed to ensure that only authorized users and devices can access an organization's IT systems and sensitive data. By implementing strong ICAM controls, HUD can minimize opportunities for adversaries to compromise user accounts, gain a foothold in systems, steal data, or launch cyberattacks. Recognizing the need to modernize Federal Government cybersecurity and to keep pace with increasingly sophisticated cyber threats, EO 14028 mandated that Federal agencies strengthen ICAM controls and advance toward a zero trust architecture (ZTA) model. Under ZTA, both users and devices are continually verified using strong authentication mechanisms. In compliance with provisions of EO 14028 and related implementing guidance within OMB M-22-09, agencies are required to progress toward ZTA by integrating strong multifactor authentication (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. HUD had made limited progress with its ICAM functions but did not have a detailed roadmap in place with plans to achieve compliance with Federal ICAM requirements, including those for MFA. As a result, while HUD remained at the defined maturity level for the ICAM domain overall, its maturity had decreased for three of the seven FISMA metrics within the domain, as shown in table 6.

Table 6. Identity and access management core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
26	(b)(5)		
27			
29			
30			
31			
32			
33			

Spotlights on Success

- With funding and support from the Technology Modernization Fund, HUD began work to expand its use of MFA.

Program Improvement Needs

- HUD had not consistently implemented MFA for privileged and nonprivileged users of its facilities, systems, and networks.
- HUD did not have timelines, budget estimates, or other details to support appropriate planning for an enterprisewide ICAM solution and implementation.
- HUD did not support that user access and activities were appropriately reviewed.

Domain Summary

HUD had made progress with its ICAM function by securing funding from the Federal Government's Technology Modernization Fund and initiating work to expand the use of MFA for one of its systems that supported approximately 15 applications. HUD's intent was to leverage this use case as a model to expand MFA across other platforms. Additionally, HUD reported that it was in the process of implementing a new privileged account management tool to expand MFA use for privileged accounts. However, despite this progress, several areas of weakness remained, and HUD faced significant challenges in achieving compliance with Federal standards and maintaining effective control over system and data access. Addressing these related weaknesses could substantially enhance HUD's ability to protect against data breaches, data integrity compromises, or system disruptions.

HUD's maturity had decreased for three of the seven metrics within the ICAM domain, primarily because HUD had not adequately planned for or implemented strong authentication mechanisms. In recent FYs, HUD has modified its strategies for an enterprisewide ICAM solution multiple times, and previous efforts have not led to successful implementation. Although HUD outlined its current plans in general terms, HUD lacked a technology solution roadmap with timelines, budget estimates, or other details for implementing an enterprise ICAM solution that included MFA. HUD reported that only 2 of its approximately 100 systems supported MFA, leaving the rest more vulnerable to unauthorized access. While additional HUD applications required users to first access HUD's network with MFA before logging in, MFA was not required at the application level, and phishing-resistant MFA factors were not consistently enforced as required under a ZTA approach. This situation increases the risk that accounts could be compromised if users are deceived into revealing their logon information.

OCIO had not annually updated its enterprise ICAM policies and procedures as required. Further, HUD system owners had not consistently reviewed and updated the security plans and documentation for their respective systems. These outdated ICAM policies and system documentation could create gaps in IT security, possibly leading to confusion among users, and an elevated risk of unauthorized access. At the enterprise level, procedures had not been updated to include (b)(5)

(b)(5)

(b)(5)

HUD also did not comply with essential requirements related to logging and account reviews. Specifically, HUD did not review privileged accounts quarterly in accordance with its policy. In the eight sample systems we reviewed, none had HUD's prescribed evidence to demonstrate that privileged accounts were appropriately restricted to eligible users. Four of the eight sample systems had evidence indicating that HUD personnel might have performed some level of user account review, such as a printed list of users. However, none of the eight systems had the review evidence prescribed by HUD's policy including before and after privileged user lists, service desk tickets for required access adjustments, and evidence of separation of duties review. Additionally, during a system demonstration provided by HUD officials, we observed that six nonprivileged user accounts were assigned privileged access, violating account separation protocols. In this instance, any account reviews performed by HUD were ineffective in ensuring that privileged access was appropriately assigned. HUD's failure to follow account separation protocols in this instance is concerning because different security controls and oversight procedures apply to privileged and nonprivileged accounts. By using nonprivileged accounts, the stricter privileged account controls can be bypassed, creating a situation in which unauthorized administrative actions could be executed without detection. Further, in seven of the eight sample systems, HUD did not demonstrate that privileged user activities had been logged and reviewed as required to detect suspicious or unauthorized activities.

HUD did not implement logging capabilities required under the four-tier maturity model (not effective, basic, intermediate, and advanced) established by OMB M-21-31. As of March 2023, HUD reported that no systems had achieved the required intermediate maturity level, and only 8 of its approximately 100 systems had achieved basic logging maturity. These deficiencies highlight a significant gap in security measures, leaving systems potentially vulnerable to undetected unauthorized activities.

Finally, HUD had not defined and maintained metrics to measure the effectiveness of ICAM program activities and assist in identifying areas for improvement. Without such metrics, HUD lacks the information necessary to identify trends that might pose potential security risks and to make informed, data-driven decisions about allocating program resources.

We offer nine recommendations and five OFIs for HUD to increase maturity in this domain. In addition, HUD has seven open ICAM domain recommendations from previous FISMA evaluation reports, as noted in appendix C.

DATA PROTECTION AND PRIVACY

Federal privacy programs are responsible for managing risks to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal (collectively referred to as “processing”) of personally identifiable information (PII) and for ensuring compliance with applicable privacy requirements. When a system processes PII, the InfoSec program and the privacy program have a shared responsibility for managing the security risks for the PII in the system.[18]

Overall, it was encouraging to see continued maturity in HUD’s privacy program, focused on the collection and use of PII. In support of its mission, HUD operates many large-scale programs designed to serve the public. The information systems supporting these programs maintained at least a billion records containing PII and daily facilitated thousands of transactions with business partners and private individuals. Although HUD’s enterprisewide privacy program made improvements in FY 2023, as noted in table 7, it needs to continue to make significant progress in allocating adequate resources to the Privacy Office, improving its removable media and sanitization processes, and implementing tools and solutions to strengthen its data exfiltration prevention and network defenses maturity.

Table 7. Data protection and privacy core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
35	(b)(5)		
36			
37			

Spotlights on Success

- HUD continued to mature its overall privacy program, including policies, procedures, roles, responsibilities, and implementation of the program across program offices.
- HUD had strengthened its network defenses and data exfiltration prevention tools and solutions.

Program Improvement Needs

- HUD did not consistently implement its digital media sanitization procedures.
- HUD did not prevent the unauthorized transfer of data to removable media.

Domain Summary

HUD continued to mature its overall privacy program as it set a baseline to implement other security controls, tools, and solutions throughout the remaining metrics within this domain. HUD defined and communicated its privacy program plan and related policies and procedures for the protection of PII that was processed by its information systems. HUD increased its awareness and visibility of privacy issues

[18] NIST SP 800-53r5, section 2.4 Security and Privacy Controls

through various forums, and they were better integrated with cybersecurity processes. Privacy was discussed during monthly privacy liaison officer (PLO) meetings with stakeholders from other program offices including OCIO and Records Management, monthly information system security officer (ISSO) forums, and in HUD's IT governance boards, such as the Technical Review Committee and Configuration Change Management Boards. The Privacy Office was staffed by the Chief Privacy Officer and six additional staff members. HUD performed a staffing analysis and determined that it needed three to six more employees to effectively implement its privacy program. In addition to the Privacy Office staff, HUD designated PLOs within each HUD program office. While HUD's Privacy Office issued policies and procedures tailored to its environment, HUD needs to continue to make significant progress to strengthen its data protection and privacy program using the tools and solutions mentioned below.

For data at rest, HUD deployed whole disk encryption for workstations on its network. For systems and applications, system owners implemented application-level encryption. However, HUD OCIO assessed system encryption controls only during the system authorization process, which was after system development. Assessing encryption controls after system development could lead to an insufficient or inappropriate level of encryption being built into the system during development, which would then require redesign, remediation, or unnecessary risk acceptance after the implementation.

For data in transit, HUD encrypted websites and web-facing applications, and HUD's internet service provider implemented security controls to secure and monitor inbound and outbound traffic to detect PII exfiltration. HUD deployed a data loss prevention (DLP) tool to scan for PII on laptops and to detect and prevent users from sending unencrypted information such as PII through email. Rulesets also monitored for externally shared PII, including Social Security numbers, bank account information, driver's license data, passport data, and taxpayer identification numbers in Office 365 files.

HUD's endpoint security solution did not prevent the unauthorized transfer of data to removable media, but it did enforce the encryption of data copied from a HUD system to removable media inserted into a workstation. Although the media were encrypted with a password, the data could still be successfully exfiltrated by a user and then subsequently transferred by external means. HUD did not exclude any type of media inserted into workstations, as there was no media whitelist or blacklist implementation.

In FY 2023, HUD implemented an endpoint detection and response solution. The solution provided DLP capabilities to discover and protect sensitive data such as PII on its endpoints, which were monitored by the Security Operations Center (SOC). HUD also implemented a solution that included DHS-provided EINSTEIN deployments for systems and enclaves at all trusted internet connection portals to collect, analyze, and share network flow data to identify network anomalies spanning the Federal Government.

Lastly, HUD should improve its implementation of its PII minimization plan, which creates and maintains the inventory of HUD's PII. The effort was developed through the privacy impact assessment (PIA) inventory, system of records notices (SORN) inventory, annual data questionnaire, coordination with Records Management, and other related efforts. However, we did not see consistent implementation of the plan at the program office level. PII minimization is critical to assist in managing the security risks for the PII in the system. HUD should collect only PII that is directly relevant and necessary to accomplish the specified purposes and retain PII only for as long as is necessary to fulfill the specified purposes.

We offer 1 recommendation and 11 OFIs for HUD to increase maturity in this domain. In addition, HUD has four open data protection and privacy domain recommendations from previous FISMA evaluation reports, as noted in appendix C.

SECURITY TRAINING

Security training encompasses 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 common attack vectors, and know how to respond to incidents. The Harvard Business Review in May 2023 estimated that, despite an exponential increase in organizational cyber training over the past decade, human error accounted for more than 80 percent of cybersecurity 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 (SAT) program can help to establish a strong culture of cybersecurity and contribute to the broader objective across all FISMA domains of safeguarding the confidentiality, integrity, and availability of HUD's information and information systems. HUD continued to consistently implement its SAT program, but areas for improvement remain to ensure program effectiveness.

Table 8. Security training core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
41	(b)(5)	[redacted]	[redacted]
42	[redacted]	[redacted]	[redacted]
43	[redacted]	[redacted]	[redacted]

Spotlights on Success

- HUD had implemented multiple cybersecurity awareness campaigns and phishing exercises designed to influence adoption of cybersecurity best practices.

Program Improvement Needs

- HUD records did not support that all users completed their required training.
- HUD did not use qualitative and quantitative performance measures to consistently gauge the effectiveness of its SAT program and demonstrate that its identified knowledge, skills, and abilities gaps were addressed through training or talent acquisition.

Domain Summary

HUD generally followed its strategy for delivering security training and assessing workforce skills. OCIO communicated with employees and contractors to outline security training requirements, maintained training completion records, and had a process to suspend network access for users who failed to complete the required training. OCIO demonstrated a commitment to improving workforce cybersecurity awareness by pursuing multiple avenues of engagement. For example, HUD conducted quarterly phishing exercises to gauge workforce cybersecurity awareness. Users who failed the exercises were targeted for additional testing and received related communications as a training tool to improve security awareness. HUD also planned and began implementing multiple cybersecurity awareness training activities designed to further influence adoption of cybersecurity best practices. Recognizing challenges in its ability to track contractor training, HUD implemented a new method for contractors to document security awareness training completion. In addition, HUD updated its metrics catalog to include measures related to cybersecurity awareness and training.

However, several areas prevented HUD from reaching the managed and measurable level for the security training domain. First, HUD did not show that resources for SAT were allocated based on risk assessments. While HUD identified funding needs for contractor support and indicated that funding was generally available to support its SAT program, it lacked budget details and information on the number of HUD personnel and contractors who perform related roles. Second, while HUD did track security awareness and specialized training completions and took action to remove network access for some users who failed to take required training, the evidence was insufficient to confirm that all users fulfilled their training obligations. This missing information includes specialized, role-based security training, for which records did not identify users who failed to take the training. HUD also did not have mechanisms to ensure that external users were held accountable for completing awareness training. Third, even though HUD took steps to identify knowledge, skills, and abilities gaps, it did not demonstrate that it had addressed the identified gaps through training or talent acquisition. Finally, although HUD collected user feedback on training courses, it did not use qualitative and quantitative performance metrics to consistently measure the effectiveness of its SAT strategy and plans.

We did not issue any new recommendations or OFIs for the security training domain in FY 2023. HUD has five open security training domain recommendations from previous FISMA evaluation reports, as noted in appendix C.

INFORMATION SECURITY CONTINUOUS MONITORING

NIST defined ISCM as "maintaining ongoing awareness of InfoSec, vulnerabilities, and threats to support organization risk management decisions."[19] HUD's ISCM strategy should coordinate efforts and implement automated tools and strategies for assessments of system controls and all other FISMA activities. This strategy would help HUD develop methods to collect, analyze, and report on agency data in a timely manner with the goal to manage risk, as appropriate, based on the organization's core missions and business processes. Overall, HUD improved its ISCM domain, as noted in table 9, restarting its ISCM and ongoing authorization (OA) program in FY 2023 after delays in its strategy and implementation plan.

Table 9. Information security continuous monitoring core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
47	(b)(5)		
48			
49			

Spotlights on Success

- HUD restarted its ISCM and OA program in FY 2023 after contract lapses due to budget constraints led to delays in its implementation plan.

Program Improvement Needs

- HUD did not hold stakeholders accountable for addressing noncritical issues identified in security and privacy assessments.

Domain Summary

Although HUD had made progress in its ISCM program, it needs to continue to enroll and authorize its systems and collect and analyze data to further mature the program. HUD's ISCM policy and strategy were issued in FY 2021, with a phased implementation approach focused on moving to OA for its systems. During FY 2023, HUD restarted its enrollment of new systems into the ISCM and OA program after delays due to budget constraints in FY 2022. The ISCM program shifted from the pilot to the implementation phase and onboarded contractor support to execute assessments. HUD's priority was to reauthorize systems with expiring authorities of operate (ATO) and enroll them into the ISCM and OA program and then begin to enroll all remaining systems in its inventory. HUD's ISCM and OA implementation plan provided key considerations and step-by-step instructions on how HUD would transition systems into its

[19] NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

OA process and grant ongoing authorizations. However, HUD did not meet its defined goal of having all systems onboarded by April 2022, as outlined in its ISCM and OA implementation plan.

While HUD continued to make progress in ongoing authorizations and assessments, it did not use the results of security control assessments and monitoring to maintain OAs of all information systems, including the maintenance of system security plans. HUD also had an ISCM control list, which defined the controls reviewed and their frequency. These controls included all security control classes, such as management, operational, and technical, as well as the types of controls, such as common, hybrid, and system specific. HUD's ISCM procedures detailed how it would operate and maintain an ISCM program at HUD to increase visibility into HUD's risks, vulnerabilities, and overall security posture annually, including developing and maintaining system security plans, monitoring controls, and time-based triggers.

Additionally, HUD's System Security Dashboard provided a clear view of vulnerabilities, up-to-date threat information, and related mission impacts for systems, such as summary information related to POA&M management, ATO artifact compliance, and ISCM assessment results. Although this dashboard collected performance measures on the ISCM program, HUD did not monitor and analyze them. The data collected in the System Security Dashboard were not updated for the first half of FY 2023 due to the lapse in contractor support and, therefore, were not monitored during that time.

Properly defined roles and responsibilities are vital to ISCM and OA success as it impacts multiple stakeholders across HUD. These roles and responsibilities were documented through HUD's ISCM and OA strategy. In that strategy, HUD described the roles and responsibilities at three tiers: organization, mission and business process, and information system. Eleven key roles were described, including the HUD CISO, the authorizing official, and the system owner, which allowed for senior-level engagement throughout the process.

While HUD did hold ISCM stakeholders accountable, it needed to address issues identified during the security and privacy control assessment. For instance, (b)(5) (b)(5) (b)(5)

We offer one recommendation and one OFI for HUD to increase maturity in this domain. In addition, HUD has one open ISCM domain recommendation from previous FISMA evaluation reports, as noted in appendix C.

INCIDENT RESPONSE

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.[20] In FY 2023, HUD continued to improve its incident response program, as noted in table 10, including its coordination with external stakeholders and incident response technologies supporting the program. These areas are key to support incident detection and analysis and effective incident response handling core metrics, as well as key Administration priorities outlined in EO 14028. Potential incidents must be detected then analyzed to determine proper communication and response actions from the appropriate stakeholders. Appropriate tools and technologies must be employed to resolve incidents in a timely manner, which requires a fully operational SOC.

Table 10. Incident response core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
54	(b)(5)		
55			
57			
58			

Spotlights on Success

- HUD achieved one of its first level 4, "managed and measurable" maturity levels because it used EINSTEIN 3 Accelerated (E3A) to detect and proactively block cyberattacks and prevent potential compromises. HUD had not previously achieved a managed and measurable level for any metric.

Program Improvement Needs

- HUD did not analyze and improve the incident response program using the captured performance measures.
- HUD had not met the event logging requirements at all three maturity levels (basic, intermediate, advanced) in accordance with OMB M-21-31.

Domain Summary

In FY 2023, HUD implemented new incident response technologies that were interoperable, covered all components of HUD's network, and collected and retained meaningful data. HUD's SOC increased visibility to cover both cloud and on-premise sources. The technologies provided HUD visibility in the form of alerts, reports, and response actions to handle potential incidents in a timely manner. However, HUD did not evaluate the effectiveness of its incident response technologies and adjust configurations and toolsets to improve its incident response detection and handling.

[20] Computer Security Incident Handling Guide (nist.gov)

HUD used E3A to detect and proactively block cyberattacks and prevent potential compromises for systems and enclaves at all TIC portals. E3A also collected, analyzed, and shared network flow data to identify network anomalies spanning the Federal Government. HUD used E3A and had DHS sensors to receive notifications through a cloud service-provided domain name system protection to screen all traffic entering and exiting its network through a TIC. (b)(5)

(b)(5)

Despite HUD's improvements to its incident response program, HUD had not met the logging requirements at all maturity levels (basic, intermediate, advanced) in accordance with OMB M-21-31.[21] Although HUD stated that it was a high priority to increase data ingestion into the security information and event management (SIEM) and meet maturity level event logging 1 within the next several months of the assessment, it was required to meet all logging requirements by August 2023.

HUD improved its SOC visibility in FY 2023 by ingesting sources from both cloud and on-premise systems. Also in FY 2023, HUD used two SIEM systems to cover its network, with one ingesting information from several cloud service providers and working toward onboarding several more. The SIEMs were HUD's main source of incident detection and analysis, which provided SOC analysts with insights that were used to create tickets and perform triage. The analysts within the HUD SOC prepared, detected, analyzed, and responded to specific types of incidents, including how it would contain, sweep, and eradicate incidents. HUD defined a common threat vector taxonomy consistent with Cybersecurity and Infrastructure Agency incident notification guidelines and developed handling procedures for specific types of incidents, as appropriate.

When an alert was triggered, the Cyber Incident Response Team analyst reviewed the alert to validate that an incident had occurred, assessed the scope, determined the attack vector, and completed an incident ticket with as much detail of the incident as possible. HUD's incident containment involved isolating threats so that they did not spread, infect, or otherwise negatively impact other areas of the HUD network.

HUD determined the stakeholders that needed to be informed of the incident following the analysis step of incident handling. HUD collaborated with DHS and other parties, as appropriate, to provide on-site technical assistance, surge resources, and special capabilities for quickly responding to incidents. HUD entered into an agreement for surge capability with the U.S. Department of Justice and leveraged DHS' U.S. Computer Emergency Readiness Team when needed to triage suspected incidents. The agreement was in the final option year, but HUD was working on establishing a new agreement. This agreement was key in addressing EO 14028 requirements for improved information sharing within the Federal Government.

We offer three recommendations and one OFI for HUD to increase maturity in this domain. In addition, HUD has six open incident response recommendations from previous FISMA evaluation reports, as noted in appendix C.

[21] M-21-31 (whitehouse.gov)

CONTINGENCY PLANNING

An effective contingency planning program ensures that plans and procedures are in place that enable systems supporting mission-essential business processes to continue operating or recover quickly and effectively following a service disruption or disaster. The first element of an effective program is to identify mission-essential functions (MEF), through the business impact analyses (BIA) process. After identifying critical systems, also known as high-value assets[22] (HVA), the second element required for an effective contingency planning program is periodic testing of the contingency plans to ensure that the plans support continuous operations and system recovery. As noted in table 11, HUD improved its contingency plan tests and exercises program in FY 2023.

Table 11. Contingency planning core and FY 2023 metric ratings.

Metric #	Metric summary	FY 2023 rating	Comparison to prior rating
60	(b)(5)		
61			
63			
65			

Spotlights on Success

- HUD demonstrated an increase in the effectiveness of its contingency plan test and exercise program, with information systems conducting annual contingency tests.
- HUD conducted a disaster recovery exercise in FY 2023 for the first time since the COVID-19 pandemic.

Program Improvement Needs

- While HUD had defined its enterprisewide business impact analysis (EWBIA), it lacked system dependencies and characterization of system components.
- HUD OCIO did not coordinate with the Office of Administration and use the results of the EWBIA to determine contingency planning requirements, including prioritizing MEFs and HVAs.

Domain Summary

In HUD's information system contingency planning (ISCP) procedures, HUD described the information that is included in a BIA, provided a mandatory template for system owners to use, and assigned responsibility to system owners to review the BIA for their system annually. In the EWBIA system prioritization analysis, HUD had a process for consolidating system-level BIA information into an EWBIA. HUD's EWBIA used a (b)(5)

[22] A High Value Asset (HVA) is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business, DHS CISA

(b)(5)

While the system-level BIAs included characterization of all system components, the EWBIA did not. The EWBIA was also incorporated into HUD's Continuity of Operations Program (COOP) for continuity and contingency planning strategy and process development, which should include identification and prioritization of MEFs and HVAs.

HUD had more consistent contingency plan testing in FY 2023. HUD's ISCP procedures and the contingency planning memorandum established an annual testing requirement, described what information was needed to develop the test plan and then conduct the test, and assigned responsibility to system owners and ISSOs to annually review the test plan and results. Additionally, HUD's ISCP testing had been integrated with the testing of other plans, such as HUD's business COOP, incident response plan, and disaster recovery exercises. In April 2023, HUD conducted the first disaster recovery test since 2019 due to the COVID-19 pandemic.

For recovery activities, HUD communicated guidance starting with the activation and notification phase. Information on the planning and performance of recovery activities was consistently communicated by OCIO to relevant stakeholders and executive management teams, which used the information to make risk-based decisions. This information included requirements to conduct annual reviews, updates, and testing of contingency plans and BIAs. The results of HUD's disaster recovery exercise were communicated regularly with relevant stakeholders, which included executive management teams.

Although HUD had more consistent communication among stakeholders regarding the results of exercises, HUD did not effectively track performance measures on the effectiveness of recovery activities and ensure that they were communicated to relevant stakeholders. HUD defined contingency planning performance measures in its Security Metrics Catalog, which was used to update HUD's System Security Dashboard. However, the dashboard was not functional for approximately half of the FY due to the loss of contractor support and, therefore, was not available to stakeholders.

We offer one recommendation and four OFIs for HUD to increase maturity in this domain. In addition, HUD has seven open contingency planning recommendations from previous FISMA evaluation reports, as noted in appendix C.

HUD'S IT BUDGET

Although not specifically assessed as part of FISMA, HUD OCIO's IT Fund has a significant influence on its FISMA maturity. HUD has reported that IT funding and resources have historically been a concern regarding cybersecurity. As HUD continues to mature its InfoSec program, more technologies, capabilities, and system modernization are required to meet Administration priorities and higher FISMA maturity levels. Additionally, many cybersecurity mandates are unfunded, which provides a unique challenge to HUD, such as the inability to use program office funds to address unfunded mandates.

HUD's limited resources is a factor that has contributed to contract lapses, with OCIO reporting the reduction or elimination of various operations and maintenance (O&M) services in previous years due to funding shortfalls. When resourcing issues occur, OCIO reportedly (b)(5) (b)(5) (b)(5). As specifically noted in the above report, data collected in the System Security Dashboard were not updated for the first half of FY 2023 due to a lapse in contractor support.

From FY 2019 to 2023, HUD ranked 20 out of 25 Chief Financial Officers Act agencies in IT funding allocated based on the overall agency budget, despite having the eighth largest budgetary resources[23] of those agencies. 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 $382 million for the FY 2023 IT fund to support the O&M of current systems and limited development, modernization, and enhancement (DME) of new initiatives. Of the $382 million in IT funds, $339 million was for continued O&M of current services, and $14 million was for continued O&M enhancements to support HUD's strategic priorities and customer needs. Only $29 million was earmarked for DME of new capabilities within OCIO and HUD's program offices, such as Federal Housing Administration and Office of Public and Indian Housing initiatives. These initiatives include continued efforts for FHA Catalyst, Native Advantage, Inventory Management and PIH Information Center, and a Grants Enterprise Management System.

[23] https://www.usaspending.gov/agency

Conclusion

According to the FY 2023 IG FISMA metrics guidance, an agency's InfoSec program is effective at level 4, "managed and measurable." HUD's InfoSec program was determined to be not effective. We assessed HUD at level 2, "defined," based on our evaluation of the 20 core metrics and 20 FY 2023 supplemental metrics within the 9 domains from the FY 2023 IG FISMA reporting guidance. Table 12 summarizes the assessed ratings of each domain and metric.

Table 12. FISMA rating summary

NIST CSF function	FISMA domain	Ad hoc	Defined	Consistently implemented	Managed and measurable	Domain maturity
Identify	Risk management	0	4	4	0	Consistently implemented
	Supply chain risk management	2	1	0	0	Ad Hoc
Protect	Configuration management	1	2	1	1	Defined
	Identity and access management	3	4	0	0	Defined
	Data protection and privacy	0	1	2	0	Consistently implemented
	Security training	0	0	3	0	Consistently implemented
Detect	Information security continuous monitoring	0	0	3	0	Consistently implemented
Respond	Incident response	0	0	3	1	Consistently implemented
Recover	Contingency planning	0	0	4	0	Consistently implemented
	Overall	**6**	**12**	**20**	**2**	**Defined**

HUD continued to take positive steps to improve its IT security posture, increasing maturity in 10 of the 40 metrics assessed in FY 2023. HUD remained at the same maturity level for 25 of the metrics and dropped in maturity for 5 metrics. These changes in maturity were consistent with HUD's progress in prior fiscal years. HUD maintained the same overall maturity level that was assessed in the FY 2022 FISMA evaluation, level 2, "defined." HUD's maturity in the FY 2023 supplemental metrics was higher than the maturity of the core metrics, which was also noted in the FY 2022 evaluation.

This report contains 23 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. implement a process to consistently update and maintain its inventory of hardware assets and ensure that the inventory is consistent with the automated discovery scans used to perform vulnerability, configurations, and continuous diagnostics and mitigation scans and

    b. use this inventory to consistently remove unauthorized hardware assets from the HUD network (IG FISMA metrics 2, 20, and 21).

2. HUD OCIO should report at least 80 percent of its government-furnished equipment through the DHS CDM program (IG FISMA metric 2).

3. HUD OCIO should

    a. implement a process to consistently update and maintain its inventory of software assets and ensure that the inventory is consistent with the automated discovery scans used to perform vulnerability, configurations, and continuous diagnostics and mitigation scans and

    b. use this inventory to consistently remove unauthorized software assets from the HUD network (IG FISMA metrics 2, 20, and 21).

4. HUD OCIO should update its software inventory policies and procedures to account for critical software as defined by EO 14028 (IG FISMA metrics 3 and 21).

5. HUD OCIO should implement policies and procedures to maintain inventories of critical software and software licenses, critical software platforms, and all software installed on critical software platforms (both critical software and noncritical software) and use the inventory of critical software platforms and all software installed on them to ensure that only supported versions of software are used on those critical software platforms (IG FISMA metrics 3 and 21).

6. HUD OCIO should

    a. in coordination with the Chief Risk Officer (CRO), document cybersecurity risk management roles and responsibilities in a consolidated list and;

    b. define procedures to hold personnel accountable to their assigned roles in the consolidated list (IG FISMA metric 7)

7. HUD OCIO should consistently implement personnel accountability procedures to ensure that assigned cybersecurity risk management roles are being performed in an effective manner (IG FISMA metric 7).

8. HUD's Office of the Chief Financial Officer (OCFO), in coordination with other appropriate program offices, should define and implement a risk-based process to assess and document IT risk management personnel resourcing needs and that those personnel are allocated effectively to support HUD's risk management program (IG FISMA metric 7).

9. HUD OCFO, in coordination with other appropriate program offices, should define and implement a process to document and allocate non-personnel risk management resources in a risk-based manner, to include but not limited to funding, processes, and technology (IG FISMA metric 7).

10. HUD OCIO should ensure that external systems, such as cloud systems and cloud service providers, have and maintain configuration management plans that are consistent with HUD's defined configuration management requirements (IG FISMA metric 19).

11. HUD OCIO should define and implement metrics to monitor the effectiveness of ICAM program activities and assist in identifying areas for improvement (IG FISMA metric 26).

12. HUD OCIO should develop a comprehensive ICAM policy, strategy, process, and technology solution roadmap, including milestones, budget estimates, and appropriate technology solution details (IG FISMA metric 27). This recommendation replaces FY 2020 FISMA recommendation 11.

13. HUD OCIO should define policies and guidance for the use of system-specific access agreements (IG FISMA metric 29).

14. HUD OCIO should develop a plan that includes milestones and funding requirements for implementing phishing-resistant MFA for all users in alignment with Federal requirements (IG FISMA metrics 30 and 31).

15. HUD OCIO, in coordination with other appropriate HUD offices, should define and communicate policies and procedures for use of MFA at HUD facilities (IG FISMA metrics 30 and 31).

16. HUD OCIO should implement procedures to ensure that digital identity risk assessments have been performed and documented in accordance with HUD's defined procedures and Federal guidelines (IG FISMA metrics 30 and 31).

17. HUD OCIO should define a plan to meet the logging requirements at all event logging maturity levels (basic, intermediate, advanced) in accordance with OMB M-21-31. This plan should include logging sufficient to allow for reviewing privileged user activities (IG FISMA metrics 32 and 54).

18. HUD OCIO should develop and implement monitoring and enforcement procedures to ensure that non-GFE devices (for example, BYOD), such as those owned by contractors or HUD employees, are either: (a) prohibited from connecting to the HUD network; or (b) properly authorized and configured before connection to the HUD network (IG FISMA metrics 2, 21, and 33).

19. HUD OCIO should develop and implement procedures and contract terms to enforce forfeiture of non-GFE devices (for example, BYOD), to allow for analysis when security incidents occur (IG FISMA metrics 33 and 55).

20. HUD's Office of Administration, in coordination with OCIO, should update and communicate its PII minimization plan. The plan should include detailed procedures to regularly review and remove unnecessary PII collections in accordance with OMB Circular A-130 (IG FISMA metric 35).

21. HUD OCIO should develop and implement processes to monitor and analyze qualitative and quantitative performance measures for the effectiveness of its ISCM program (IG FISMA metric 47).

22. HUD OCIO should define a process and assign responsibility to evaluate the effectiveness of its incident response technologies and adjust configurations and toolsets to improve the incident response program (IG FISMA metric 58).

23. HUD OCIO should update its enterprisewide business impact prioritization analysis procedures to include system dependencies and the characterization of system components (IG FISMA metric 61).

Appendixes

APPENDIX A – AGENCY COMMENTS AND OIG'S RESPONSE

Agency Comments

HUD OCIO stated it did not have any formal comments on the draft report. OCIO did provide technical comments that OIG incorporated into the final report.

OIG Response

HUD OCIO stated it did not have any formal comments to the draft report. OIG incorporated HUD OCIO's technical comments into the final report.

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.[24] The scope of our review was department-wide, resulted in conclusions and recommendations made at the Department level, and covered the period October 1, 2022, to September 30, 2023.[25]

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.[26] 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 Metrics[27] and associated CyberScope reporting questions. We assessed the core metrics and the FY 2023 supplemental metrics for a representative 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 IG 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 InfoSec, 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.

We evaluated the following organization levels to accomplish our objectives:

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

[25] This narrative report is based on our CyberScope report in Appendix F, which was issued August 28, 2023.

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

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

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 2023 supplemental metrics across eight program office systems, which are listed in table 13 below.

Table 13. Systems assessed using IG FISMA metrics

System code	Program office	System name	Acronym	Mission critical	Security financial PII	Type
A75R	(b)(5)					
P326						
P295						
P321						
P202						
P162D						
P303						
P323G						

Sample System Descriptions from HUD’s IAS

(b)(5)

System Technical Description:

(b)(5)

(b)(5)

(b)(5)

Reporting

We compiled the information necessary to address the specific reporting requirements outlined in OMB M-23-03, FY 2023 Guidance on Federal Information Security and Privacy Management Requirements.[28] Responses to specific IG FISMA reporting metrics were submitted through the DHS web-accessible CyberScope application.

Penetration Testing

Finally, we conducted penetration testing in accordance with FISMA guidance on the selected sample systems' infrastructure servers and web applications, as applicable. Penetration testing also included the internet, intranet, the Denver field office WiFi network, and local area network general support systems in scope. 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.

[28] M-23-03-FY23-FISMA-Guidance-2.pdf (whitehouse.gov)

APPENDIX C – SUMMARY OF PRIOR FISMA RECOMMENDATIONS

The U.S. Department of Housing and Urban Development (HUD) Office of Inspector General has issued 248 recommendations in our prior annual Federal Information Security Modernization Act of 2014 (FISMA) evaluation reports since Fiscal Year (FY) 2013. All recommendations from the FY 2013, FY 2014, and FY 2016 reports have been closed. Of the 248 recommendations, 58 were still open as of September 30, 2023. This appendix describes the status of the FISMA recommendations in detail. Table 14 shows the distribution of the 58 open recommendations by domain and by the FY in which the recommendation was issued. Figure 3 shows the distribution of open recommendations by the FY in which the recommendation was issued.

Table 14. FISMA evaluation open recommendations by domain (FY 2015-2022)

Domain	FY 2015	FY 2017[29]	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	Domain total
Risk management	(b)(5)							
Supply chain risk management[30]								
Configuration management								
Identity and access management								
Data protection and privacy								
Security training								
InfoSec continuous monitoring								
Incident response								
Contingency planning								
Fiscal year total								

[29] As noted above, all FY 2016 recommendations have been closed, so this FY is omitted from all tables and figures in this appendix.

[30] Supply chain risk management was first created as a domain in FY 2021.

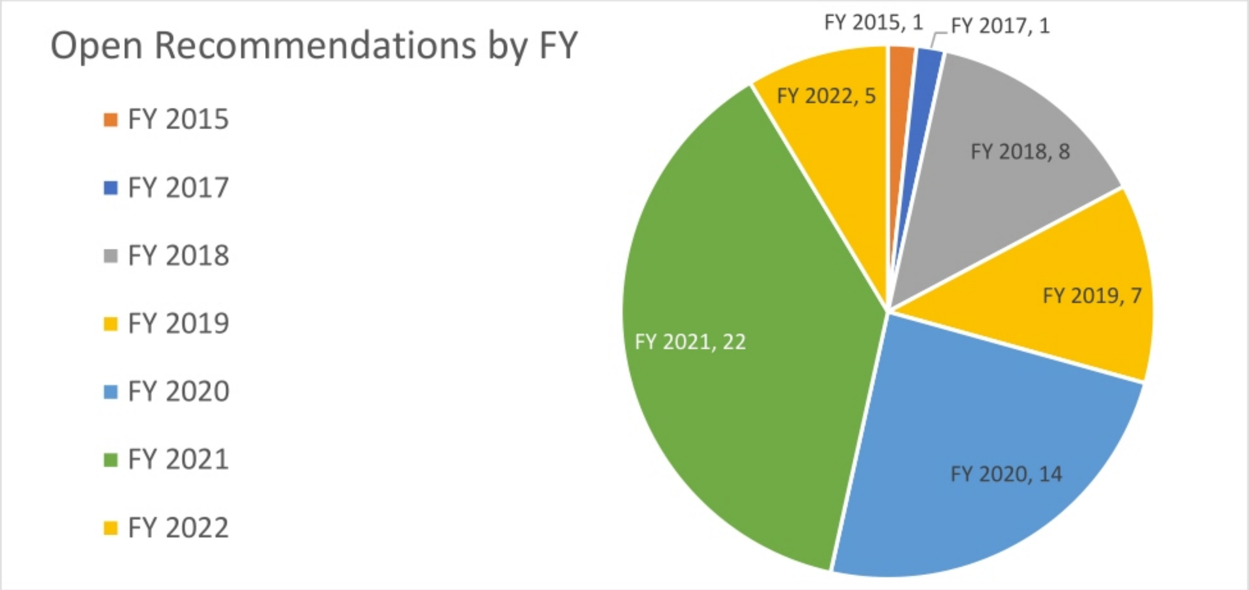


Figure 3. FISMA evaluation open recommendations by FY

HUD made progress in closing recommendations in FY 2023. Overall, 77 percent of our FISMA recommendations have been closed since FY 2013. 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.

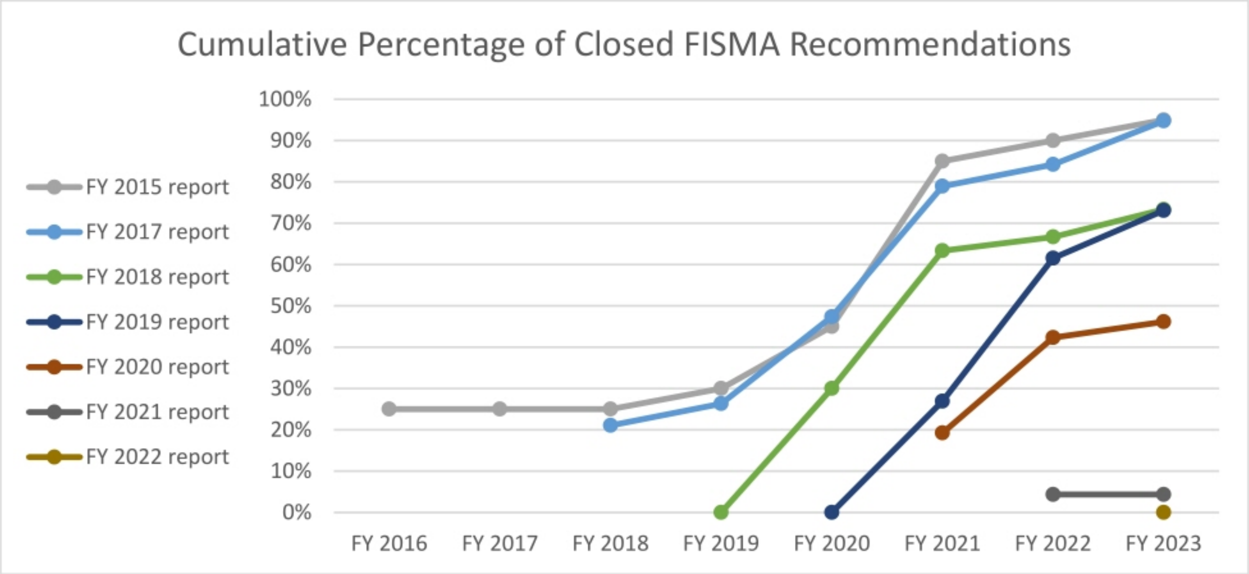


Figure 4. FISMA evaluation recommendation cumulative closure percentage by FY

Finally, table 15 shows HUD's progress in closing recommendations. In FY 2023, HUD closed 9 FISMA recommendations, which represented a seventh of the open FISMA recommendations. Additionally, HUD closed 1 recommendation at the end of FY 2022 that was not credited in that evaluation. As HUD's Office of the Chief Information Officer and Office of Administration address the remaining open recommendations, HUD will make progress towards improving the maturity of its InfoSec program.

Table 15. FISMA evaluation recommendation closure status

Fiscal year	Total number of recommendations	Number of open recommendations	Number of closed recommendations	Recommendations closed in FY 2023
2013	62	**All recommendations (62) closed as of FY 2022**		
2014	23	**All recommendations (23) closed as of FY 2021**		
2015	20	1	19	1
2016	14	**All recommendations (14) closed as of FY 2022**		
2017	19	1	18	2
2018	30	8	22	2
2019	26	7	19	3
2020	26	14	12	1
2021	23	22	1	0
2022	5	5	0	0
FY totals	**248**	**58**	**190**	**9**

APPENDIX D – OPPORTUNITIES FOR IMPROVEMENT

For the FY 2023 FISMA evaluation, we provided HUD with 66 opportunities for improvement (OFI). These issues will not be tracked as formal recommendations but are noted as general suggestions to improve the effectiveness of the U.S. Department of Housing and Urban Development's (HUD's) InfoSec program implementation. OFIs are presented at both the enterprisewide and system level. System-specific OFI's were developed based on our evaluation of selected security controls for a sample of HUD program offices.

APPENDIX E – LIST OF ABBREVIATIONS

Acronym	Definition
BIA	business impact analysis
CDM	continuous diagnostics and mitigation
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
COOP	Continuity of Operations Program
CSAM	Cyber Security Assessment and Management
CSF	Cybersecurity Framework
DHS	U.S. Department of Homeland Security
DLP	data loss prevention
DOJ	U.S. Department of Justice
EDR	endpoint detection and response
EO	executive order
ERM	enterprise risk management
EWBIA	Enterprise-wide BIA
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
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
IR	incident response
InfoSec	information security
ISCM	information security continuous monitoring

ISCP	information system contingency plan
ISSO	information system security officer
IT	information technology
MEF	mission-essential function
NIST	National Institute of Standards and Technology
OA	ongoing authorization
OCIO	Office of the Chief Information Officer
OCPO	Office of the Chief Procurement Officer
OFI	opportunity for improvement
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
PLO	privacy liaison officer
POA&M	plan of action and milestones
SCRM	supply chain risk management
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOP	standard operating procedures
SORN	system of records notice
TIC	Trusted Internet Connection

APPENDIX F – FY 2023 HUD OIG CYBERSCOPE SUBMISSION

The inserted document below contains the Inspector General (IG) responses to the fiscal year (FY) 2023 IG Federal Information Security Modernization Act of 2014 (FISMA) metrics, established by the Office of Management and Budget (OMB). OMB issued Memorandum 23-03, FY 2023 Guidance on Federal Information Security and Privacy Management Requirements, on December 2, 2022. The memorandum details required FISMA reporting instructions. The document below was submitted to the Department of Homeland Security's (DHS's) CyberScope portal on August 28, 2023.

APPENDIX G – ACKNOWLEDGEMENTS

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

Major Contributors

Randy D. Jackson, Assistant Director, project supervisor
Kirk Van Camp, Senior IT Evaluator, project team lead
David Torre, Senior IT Evaluator
Blake Hayes, IT Evaluator