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

HUD Fiscal Year (FY) 2026 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation

Report Number: 2027-OE-0001

October 30, 2026

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

The following record is a HUD OIG document. The redactions applied within this document 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.

Highlights

HUD Fiscal Year (FY) 2026 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation| 2027-OE-0001

What We Evaluated and Why

We reviewed 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 each Office of Inspector General (OIG) to conduct an evaluation of its agency's InfoSec programs and practices. For the Fiscal Year (FY) 2026 assessment, the Office of Management and Budget (OMB) and the Cybersecurity Infrastructure Security Agency (CISA) instructed agencies to use the FY 2025 Inspector General (IG) FISMA metrics which consisted of 20 core metrics and 5 supplemental metrics. We assessed the effectiveness of HUD's InfoSec program on a metric maturity model that ranges from maturity level 1, ad hoc, to maturity level 5, optimized.

What We Found

HUD's InfoSec program remained ineffective at level 3, although it continued to mature its program in FY 2026. OMB guidance states that maturity level 4, managed and measurable, is an effective level of maturity, which means that level 3 is ineffective.

In FY 2026, HUD focused on developing a few key initiatives. First, the Office of the Chief Information Officer (OCIO) made significant progress with its enterprise identity and access management program which will implement phishing resistant multifactor authentication across the agency. OCIO developed solutions to include legacy systems and rolled out the program to tens of thousands of internal and external users. Second, OCIO implemented updated governance structure to increase accountability through collaboration and modern information technology (IT) development methodologies. Lastly, HUD improved its system and environment monitoring capabilities and visibility through dashboards.

However, in FY 2026, HUD faced InfoSec challenges in some program areas. First, HUD allowed approximately (b)(5) systems to continue to operate with expired authorization to operate (ATO) certificates which created additional cyber risk. Second, HUD's data governance program remained in its early stages of development, which limited HUD's ability to implement secure data management practices. Third, OCIO maintained (b)(5) open risk management recommendations, which must be resolved to mature the risk management program. Lastly, OCIO reported a challenge with maintaining an adequate level of technical staffing, therefore, limiting OCIO's capacity to advance initiatives.

What We Recommend

This report contains four recommendations to improve HUD's InfoSec program. The recommendations are to guide HUD to the next maturity level and to address identified weaknesses at the lower maturity levels that still exist. The recommendations address gaps in the configuration management, security training, information systems continuous monitoring (ISCM), and incident response (IR) domains, including improving scanning capabilities, collecting security training performance measures, and adding automation to ISCM and IR programs.

Table of Contents

Background and Objectives 1

Results of Evaluation 4

HUD's Information Security Program Remained Ineffective 4

Scope and Methodology 14

Appendix A – Prior FISMA Recommendations 16

Appendix B – Management Response 17

Appendix C – FY 2026 HUD OIG CyberScope Submission 24

Appendix D – FISMA Metric Trends 25

Background and Objectives

The objective of this evaluation was to assess the maturity level of the U.S. Department of Housing and Urban Development's (HUD) information security (InfoSec) program and practices in accordance with the Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) metrics.

Specific objectives of this evaluation included:

- Performing the annual independent evaluation of the effectiveness of HUD's InfoSec program and practices as required by FISMA.[1]
- Testing the effectiveness of HUD's InfoSec policies, procedures, and practices through the analysis of a selection of HUD's information technology (IT) systems, which are labelled as "sample systems" in this evaluation report.
- Assessing the maturity level of HUD's InfoSec program and practices using the results of sample system testing and enterprise information collected from HUD's Office of the Chief Information Officer (OCIO) against the FY 2025 IG FISMA Reporting Metrics for the FY 2026 independent evaluation.[2]
- Preparing responses for each applicable Office of Management and Budget (OMB)/Department of Homeland Security (DHS) CyberScope IG FISMA metric, with the support and conclusions documented for each response.

FISMA requires all IGs to assess the effectiveness of the InfoSec program of its respective Federal agency on an annual basis. OMB, DHS, and the Council of Inspectors General on Integrity and Efficiency (CIGIE) coordinate to develop IG FISMA metrics required to be assessed each FY. For the FY 2026 evaluation, IGs were instructed to utilize the FY 2025 IG FISMA metrics. The IG FISMA metrics were assessed using a maturity model described below.

IGs were required to submit the results of their annual FISMA assessments through the DHS-hosted CyberScope reporting application, which recorded individual responses to the IG FISMA metrics. Each of the metrics was associated with a domain and a function, as described below. Consistent with OMB guidance, the HUD Office of the Inspector General (HUD OIG) has also developed this narrative report summarizing the results of our FISMA assessment, and this report includes our recommendations to HUD to improve its InfoSec program.

FISMA Overview

The Federal Information Security Management Act of 2002 (Public Law 107-347), as amended by FISMA (Public Law 113-283), establishes the following responsibilities for agency heads:

- Providing appropriate InfoSec protections to maintain the confidentiality, integrity, and availability of the agency's information and the systems containing and processing that information.
- Ensuring compliance with the requirements of FISMA; OMB policies; and National Institute of Standards and Technology (NIST) policies, procedures, standards, and guidelines.

[1] Public Law 107–347 (https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf) and Public Law 113-283 (https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf).
[2] FY 2025 IG FISMA Reporting Metrics v2.0 (April 3, 2025). https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf.

- Ensuring that InfoSec management processes are integrated with agency strategic and operational planning processes.
- Ensuring that senior agency officials provide InfoSec for the information and information systems that support the operations and assets under their control.
- Ensuring that all personnel are held accountable for complying with the agencywide InfoSec program.

IG FISMA Metrics

On March 17, 2026, CISA notified IGs to utilize FY 2025 IG FISMA Metrics for the FY 2026 evaluation, which included a total of 25 metrics for IGs to assess. The metrics were divided into two categories, as follows:

- 20 core metrics, which have been assessed by OIGs annually since FY 2022; and
- 5 supplemental metrics, which were first assessed in FY 2025.

OMB selected the 20 core metrics in FY 2022 to represent a combination of high-impact security processes and essential functions necessary to determine the overall effectiveness of the InfoSec program. The core metrics were primarily chosen to align with Executive Order (EO) 14028, titled "Improving the Nation's Cybersecurity."[3] Since we have assessed the same core metrics each year since FY 2022, HUD's historical scores in the core metrics show the change in the maturity of its InfoSec program over time. The trend of improving scores in the core metrics since FY 2022 reflects the overall improvement of the InfoSec program over that time frame. We provide more information about HUD's scoring in the core metrics below in the results of our evaluation and in Appendix D.

Table 1 – NIST Cybersecurity Framework (CSF) 2.0[4] function and FISMA domain alignment

NIST CSF 2.0 Function	FISMA Domain
Govern	• Cybersecurity Governance • Cybersecurity Supply Chain Risk Management
Identify	• Risk and Asset Management
Protect	• Configuration Management • Identity and Access Management • Data Protection and Privacy • Security Training
Detect	• InfoSec Continuous Monitoring
Respond	• Incident Response
Recover	• Contingency Planning

[3] EO 14028, "Improving the Nation's Cybersecurity" (May 12, 2021). https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.
[4] NIST CSF 2.0. https://www.nist.gov/cyberframework.

Metric Maturity Model

The IG FISMA metrics used a five-level maturity model ranging from ad-hoc at the lowest level to optimized at the highest level. We assessed the IG FISMA metrics by using specific criteria that OMB provided in the FISMA guidance to establish the maturity level rating of each metric. Further, each domain and NIST CSF 2.0 function have an assessed maturity level based on the scores of the underlying metrics in that domain or function, respectively. Finally, HUD's overall InfoSec program has an assessed score based on the combined results of the six NIST CSF 2.0 functions. According to OMB and DHS guidance, maturity level 4, managed and measurable, generally represents an effective level of maturity. Figure 1, below, shows an overview of the FISMA maturity model.

Figure 1 – FISMA maturity model levels



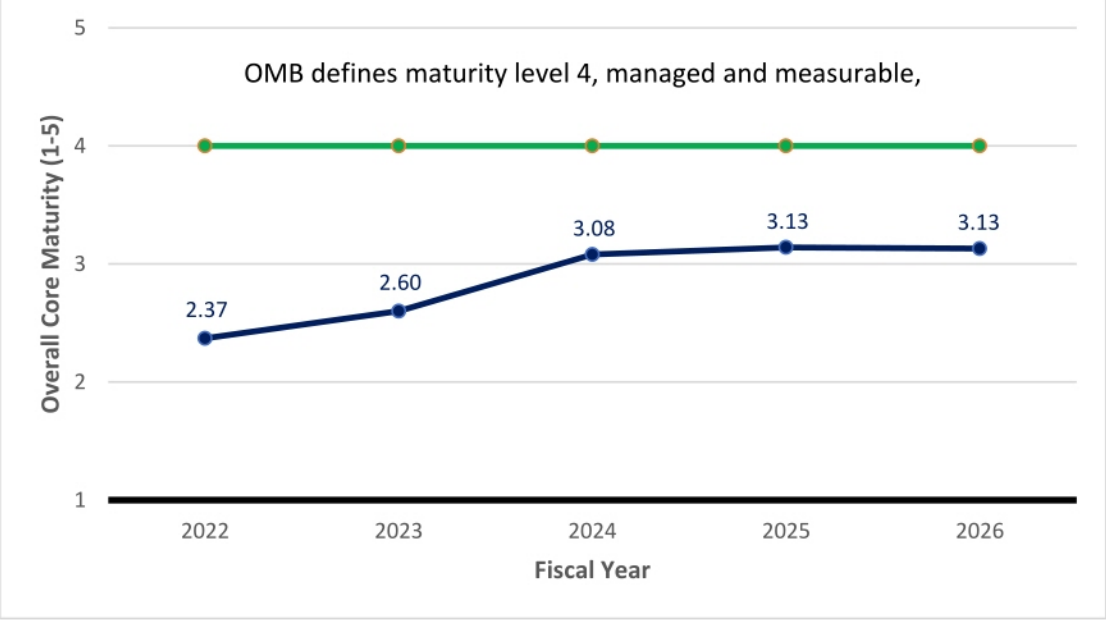
Results of Evaluation

HUD's Information Security Program Remained Ineffective

In FY 2026, we assessed HUD at maturity level 3, consistently implemented, for its overall InfoSec program. OMB guidance states that maturity level 4, managed and measurable, is an effective level of maturity, which means that level 3 is ineffective. HUD improved maturity in metric 27 and metric 30 for the information systems continuous monitoring (ISCM) and incident response domains. HUD also decreased in maturity in metric 28 for the ISCM domain. HUD maintained its maturity for the other 18 core metrics and 4 supplemental metrics. In addition to these specific metric changes, HUD made improvements in additional InfoSec initiatives including its Enterprise Identity, Credential, and Access Management (eICAM) program, governance and accountability, and monitoring, visibility and dashboards. Furthermore, HUD faced challenges in the areas of expired Authorizations to Operate (ATOs) and ISCM program implementation, data governance, risk management, and technical staffing. Improvement in these areas, along with implementing the corrective actions of the 41 open FISMA recommendations, would address gaps in HUD's FISMA maturity. Refer to Appendix A for a listing of open recommendations by FISMA domain.

OMB selected 20 core metrics that represented high-impact security processes and essential functions in FY 2022. HUD scored the same in the core metrics in FY 2026 as it did in FY 2025, with improvement in some areas and challenges in others. We provided HUD with the annual CyberScope report on July 30, 2026, which further details our assessment of the 25 FISMA metrics.[5] However, HUD continued to mature its InfoSec program in areas that were not reflected in the core metrics since FY 2022. Figure 2 below shows HUD's historical core metric maturity rating since FY 2022.

Figure 2 – HUD's progress in core metric maturity since FY 2022



[5] The OIG has determined that the contents of this report would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.

Table 2 below summarizes the number of metrics assessed at each maturity level by FISMA domain and the assessed ratings of each domain and metric.[6]

Table 2 – Summary of FISMA metrics by function and domain

NIST CSF 2.0 Function	FISMA domain	Defined (2)	Consistently implemented (3)	Managed and measurable (4)	Domain maturity
Govern	Cybersecurity governance	0	3	0	Consistently implemented
	Cybersecurity supply chain risk management	0	1	0	Consistently implemented
Identify	Risk and asset management	2	4	0	Consistently implemented
Protect	Configuration management	0	2	0	Consistently implemented
	Identity and access management	2	1	0	Defined
	Data protection and privacy	0	1	1	Managed and measurable
	Security training	0	0	1	Managed and measurable
Detect	InfoSec continuous monitoring	1	1	1	Consistently implemented
Respond	Incident response	0	0	2	Managed and measurable
Recover	Contingency planning	0	1	1	Managed and measurable
Overall		**5**	**14**	**6**	**Consistently implemented**

Spotlights on Key Initiatives

Enterprise Identity and Access Management Development

OCIO improved HUD's identity management program as one of its largest initiatives in FY 2026. OCIO recognized identity management as one of its most challenging areas of information security and developed an eICAM plan to help the agency mature. Historically, identity and access management is the FISMA domain with the lowest maturity. The eICAM program is a large undertaking by OCIO that requires rebuilding system environments, developing application program interfaces (APIs), onboarding approximately (b)(5) systems that are structurally different, and developing rollout plans so users do not have interruptions in service. In FY 2025, OCIO surveyed personnel from all systems to ensure it developed an eICAM program that operated effectively across all systems. OCIO then developed a rollout plan and deployed a pilot program for its eICAM solution to (b)(5) (b)(5) n FY 2026 based on the information it received from its survey responses.

[6] No metrics were scored at either level 1, ad-hoc, or level 5, optimized.

OCIO onboarded approximately (b)(5) internal and external users to its eICAM program through the pilot program. This pilot included phishing resistant multifactor authentication (MFA) and new identity management processes. External users experienced several onboarding challenges. OCIO used that information to guide subsequent rollouts. Additionally, OCIO developed and tested an API integration between two separate programs for digital identity proofing, which was among the first of its kind across Federal agencies. This capability enables modern, risk-based identity verification and allows HUD to move away from reliance on social security numbers (SSNs) for identity proofing, resulting in a key privacy and security improvement.

The next step of HUD's eICAM rollout was onboarding HUD's (b)(5) which serves as the authentication platform for approximately (b)(5) HUD systems. This system is a legacy authentication system for HUD and required a unique approach to ensure it fits in with HUD's eICAM program. This started with developing a new unified landing page for (b)(5) n FY 2026 designed to streamline user access and support MFA and eICAM enrollment. This portal will become the single-entry point for both internal and external users, addressing legacy challenges and improving integration across platforms. The onboarding of (b)(5) systems is being conducted systematically, with a focus on ensuring all systems benefit from centralized identity management.

A central component of this modernization is the development of a unified user registration process that establishes one identity for all HUD systems, enabling consistent identity lifecycle management across internal and external populations. In FY 2026, HUD began building centralized identity governance frameworks to ensure consistent and standardized identity services across the enterprise. This enterprise identity fabric will provide a centralized view of identity, allowing HUD to enforce role based and attribute-based access controls (RBAC/ABAC) directly within HUD's architecture rather than relying on each system to develop individual access roles. HUD expects this shift to enhance security consistency, reduce the outstanding issues caused by older systems, and strengthen policy governance across the enterprise. HUD's goal for full enterprise adoption of the eICAM program is at the (b)(5) HUD still needs to onboard hundreds of systems with their own unique challenges to reach this goal; however, in FY 2026, it continued to make significant progress on its eICAM program.

A robust eICAM program is critical in today's IT landscape because it establishes strong, centralized control over who can access what within an organization's systems. By ensuring that identities are verified, privileges are properly assigned, and access is continuously monitored, eICAM significantly reduces opportunities for unauthorized access, data leakage, and attackers moving into other parts of the network during cyber incidents. It also strengthens resilience by enforcing consistent security policies across diverse environments, supporting rapid response to threats, and enabling organizations to maintain the integrity and confidentiality of their information assets.

OCIO Governance and Accountability

Another OCIO initiative in FY 2026 was to strengthen governance and accountability across its IT programs. Leadership recognized that historically IT development and management faced challenges with contractors on missed milestones, prompting OCIO to foster a culture of accountability by establishing clearer expectations.

In OCIO's FY 2026 – FY 2030 Strategic Plan, it noted a goal to centralize technology from across the department into OCIO. OCIO also planned to centralize information system security officer functions into OCIO for better governance capabilities. In addition, HUD began developing smaller, more focused policies to make standardized requirements easier for staff to follow and to enable leadership to hold

teams and contractors accountable for measurable outcomes. The department also leveraged project management tools to provide leadership with real-time visibility into project progress and accountability, supporting more effective oversight and timely intervention. The dashboard will track the status of all IT projects and monitor budget utilization, an area that had historically lacked sufficient visibility. Project information will be captured, allowing the dashboard to generate daily reports as project teams update project information. The tool is expected to provide leadership with timely insight into project performance, budget execution and overall project status, enabling more informed decision making and strengthening oversight of HUD's IT portfolio.

One of HUD's ongoing initiatives to implement more accountability through governance was to shift to a Development, Security, Operations (DevSecOps) development methodology for a more standardized IT environment. This approach builds software in a way where security, teamwork, and continuous improvement are built in from the start rather than added on later. To support this initiative, the agency began to restructure portions of its environment to move away from legacy IT, which historically made it difficult to add modern security practices. HUD began a project to implement standardized development practices throughout the agency that supported more predictable change management practices and improved the ability to modernize systems as needed. By embedding security checks directly into development workflows and expanding dashboard visibility into IT projects, HUD strengthened its ability to detect risks earlier in the lifecycle, timely meet milestones, and reduce the buildup of legacy system issues across the enterprise. A true DevSecOps environment will allow the agency to become more agile with necessary IT improvements, changes, and modernization with security at the forefront of the environment.

These efforts, combined with the implementation of a unified governance framework and the promotion of directly responsible individuals for each project, reflect HUD's commitment to building a new IT culture to support a transparent and results-driven organization.

Monitoring, Visibility, and Dashboards

In FY 2026, HUD improved its visibility in both IT and cybersecurity activities, including monitoring and detection capabilities to identify threats. HUD also worked to develop dashboards to improve executive reporting, automate data collection and provide leadership with more comprehensive insights into the organization's cybersecurity posture.

Expanding Enterprise Threat Monitoring Capabilities

HUD continued to improve how it responds to incidents through its Security Operations Center (SOC) monitoring capabilities, which helps identify potential threats and vulnerabilities. This included integrating cyber threat intelligence into its Security Information and Event Management (SIEM) platform, enabling the automated connection of security events with thousands of known signs of an attack. When automated alerts identified suspicious activity, SOC analysts performed additional investigations to validate findings and assess potential risk. The SOC also monitored threat actor trends and provided leadership with routine intelligence briefings, enabling more informed risk-based decision making. To further strengthen enterprise monitoring, HUD integrated Network Access Control logs into the SIEM environment. This enhanced OCIO's ability to correlate device activity across multiple security tools and improve enforcement of network access controls. The expanded use of automated threat intelligence enhanced behavioral analytics, increased OCIO's ability to proactively identify cybersecurity threats and respond more effectively. Additionally, to improve visibility across the enterprise, OCIO implemented user and entity behavior analytics capabilities to establish behavior profiles for users and network activity.

These capabilities enabled OCIO to develop activity baselines and more effectively detect anomalous behavior that may indicate unauthorized access or other malicious activity. OCIO also deployed monitoring capabilities to identify unusually large file transfers, improving its ability to detect potential data exfiltration and safeguard sensitive information.

Dashboards Improvements

In addition to strengthening monitoring capabilities, HUD enhanced its operational oversight by implementing real-time security dashboards and developing a standardized catalog of performance metrics. These tools provide leadership and security personnel with timely insight into key operational indicators, enabling more informed decision making and improved visibility into the effectiveness of incident response activities.

OCIO further matured its incident management process by integrating incident tracking and workflow management into a dashboard, providing more consistent and structured approach to managing cybersecurity events. OCIO also began measuring the quality of its detection capabilities by tracking both true positive and false positive incident rates. These performance measures allow OCIO to qualitatively and quantitatively assess the effectiveness of its incident detection and analysis process while using the results to identify opportunities of continuous improvement. The dashboard added the capability for leadership to have a clear view of OCIO's incident response program.

OCIO also initiated efforts to modernize its continuous diagnostics and mitigation (CDM) dashboard to improve visibility into the organization's cybersecurity posture. In FY 2026, the CDM dashboard was not fully implemented, but HUD improved its capability of accurately ingesting system information. The CDM will provide a more complete and accurate view of HUD's systems by consolidating data from multiple security tools into a single platform. The CDM will integrate information from multiple sources, allowing security information to be collected automatically rather than through manual processes. Once completed, the enhanced CDM dashboard is expected to provide leadership with a centralized view of the organization's security posture, including key performance measures such as vulnerability remediation timelines. The dashboard will also provide OCIO with a live view of FISMA performance metrics and automate much of the reporting currently performed manually. In addition, the dashboard is expected to incorporate CDM rapid response capabilities including threat hunting information and guidance on making systems tougher to break into, providing leadership with timelier information to support cybersecurity operations and risk-based decision making.

Collectively these initiatives reflected HUD's broader effort to improve organizational visibility by automating data collection, enhancing reporting capabilities, and providing leadership with more timely and actionable information. Once fully implemented, these efforts are expected to strengthen executive oversight, improve operational decision making and support more effective management of HUD's IT and cybersecurity programs.

Program Improvement Needs

HUD faced some longstanding InfoSec programmatic challenges in the areas of security authorizations, data protection, risk management, and technical staffing. Additionally, we identified new metric gap challenges resulting from changes in security control implementation directly associated with individual metrics. We issued four new recommendations to address these gaps.

Expired Authorizations to Operate (ATOs) and Lack of Information Systems Continuous Monitoring (ISCM) implementation

HUD implemented an Information Systems Continuous Monitoring (ISCM) program that divided security control families into thirds, allowing each enrolled system to assess one-third of its controls annually rather than conducting full assessments every three years under the traditional Authorization to Operate (ATO) process. However, HUD faced ongoing challenges in applying this approach across the enterprise. Implementation remained inconsistent. The ISCM program was paused for FY 2025 and restarted in FY 2026, with only (b)(5) systems enrolled in the ISCM program. This indicates HUD was unable to demonstrate that system-level continuous monitoring strategies were consistently applied across the enterprise. From an enterprise perspective, an agency-wide ISCM program relies on data from all systems. Limited participation results in potential security blind spots and makes it difficult to make ongoing, accurate risk assessments on HUD's overall InfoSec program.

(b)(5)

Additionally, many of HUD's systems continued to rely on NIST SP 800-53 Revision 4 security control baselines rather than transitioning to the current Revision 5 requirements. NIST 800-53 Revision 5 was published in FY 2020 and Revision 4 was formally withdrawn in FY 2021, yet HUD had not completed its transition in FY 2026. This misalignment limited HUD's ability to demonstrate that system-level continuous monitoring strategies and associated processes were implemented consistently across its environment. The low program participation rate, outdated security control baselines, and the high number of expired ATOs collectively restricted HUD's ability to maintain current security documentation, conduct ongoing assessments of management, operational, and technical controls, and sustain a comprehensive view of the agency's security posture.

Data Program

In FY 2026, HUD established a data governance program, yet the program remained in its early stages. The Chief Data Officer (CDO) led HUD's enterprise data governance efforts, with an emphasis on establishing department-wide data visibility, strengthening data management practices, and building a foundation for future analytic capabilities. The program is progressing toward a more structured and coordinated enterprise data governance model, supported by governance bodies and policy development.

HUD established a multi-layered governance model. This model included a Data Governance Board comprising of all General Deputy Assistant Secretaries as the representative from every program office and a Senior Data Council made up of program office data stewards, typically the data owners, and others involved in the data management program. The data governance board is working on updating the data management lifecycle and the enterprise data management policies.

The CDO's largest initiative in FY 2026 was an enterprise data catalog. The rollout will follow a (b)(5) (b)(5) (b)(5) A key challenge for the initiative is HUD's vast systems and interconnectivity of systems, which will require close coordination with OCIO. The vision for the catalog is to support an enterprise data platform, improve data trust and transparency, and enable department-wide analytics. HUD had not yet completed the (b)(5) (b)(5) which the OIG issued a priority recommendation for in the U.S. Department of Housing and Urban Development Personally Identifiable Information Risk Management in a Zero Trust Environment (2023-OE-0007) Evaluation Report in 2024.[7] Until this is complete, HUD lacks true visibility into its data and its movement. A lack of (b)(5) makes it difficult for an agency to successfully use other security tools, since most automation and monitoring rely on (b)(5) It also significantly increases security risks because sensitive information may be mishandled or exposed. Without (b)(5) proper access controls can't be implemented, leading to inconsistent or overly broad data access. Overall, the agency loses visibility and control over its information environment. Mature programs can track data throughout their systems and entry and exit points based on (b)(5) which also allows for more advanced automated tools to be deployed to prevent data loss, data breach, and other types of cyber-attacks.

HUD reported that resources, such as funding and personnel for the data governance program are limited. The CDO's budget resides in the Office of Policy Development and Research, yet the role of the CDO resides within OCIO. Funding only covered contractor support through August 2026. The CDO is reliant on contractor support to finish the data catalog. Lastly, there were also only approximately 1.5 full-time employees dedicated to data governance operations. The success of HUD's enterprise data governance program depends heavily on active participation from program offices. While some offices demonstrate strong engagement, others are still adapting to governance expectations, emphasizing the need for cultural change and a shift away from siloed data practices. Without appropriate resources, HUD cannot improve its data governance program. This limited HUD's ability to mature in areas of governance, risk, access, and data protection and privacy, which are reliant on the ability to follow data throughout its environment.

Risk Management Challenges

HUD remained at the same maturity level in the risk and asset management domain in FY 2026 and maintained (b)(5) open recommendations associated with this domain. OCIO serves as the stakeholder responsible for identifying and managing cybersecurity and IT risks and maintains the responsibility of elevating cyber risks to the enterprise risk program as needed. A centralized approach to risk management allows an organization to prioritize resources, evaluate risk tradeoffs, and make informed enterprise-wide risk management decisions. HUD did not close any risk and asset management recommendations in FY 2026. While the program faced challenges in FY 2026, the OIG did not issue additional risk and asset management recommendations, as the department should address the (b)(5) current open recommendations to mature this domain.

Additionally, OCIO lacked a governance, risk, and compliance (GRC) tool, which limited its ability to organize, prioritize, and manage cybersecurity risks. A GRC tool centralizes policy enforcement, control documentation, continuous monitoring, and audit readiness, which enables agencies to maintain visibility

[7] US Department of Housing and Urban Development Personally Identifiable Information Risk Management in a Zero Trust Environment

into risks and demonstrate compliance via NIST-based frameworks. Without a GRC tool, organizations often suffer from fragmented processes, manual record-keeping, and dangerous compliance blind spots, making it difficult to proactively manage evolving threats and increasing the likelihood of audit findings, regulatory penalties, and costly security incidents.

Technical Staffing

A recurring theme for FY 2026 was the significant work force challenges facing OCIO. Staffing levels remained below 50 percent of approved positions, creating expertise gaps across several critical IT functions. The staffing shortage limited HUD's ability to execute strategic initiatives, oversee technology projects and maintain essential operational capabilities.

The prolonged reliance on contractors presented additional challenges. Over time, much of HUD's technical expertise had become concentrated within contractor personnel rather than the federal workforce, limiting institutional knowledge and reducing government visibility into key systems and operations. As part of its workforce strategy, the CIO planned to (b)(5) (b)(5) At the same time, leadership reassessed existing contractor support to ensure contracts aligned with OCIO priorities. Contractors that did not meet performance expectations or achieve contract objectives were identified for replacement and leadership reported that future contracts would include strengthened performance requirements and accountability measures to better ensure organizational needs were met.

The staffing shortages also affected technology management and modernization efforts. OCIO reported that developers had previously been permitted to design and build systems with limited architectural oversight, resulting in inconsistent development practices. OCIO also acknowledged that Information Technology Project Managers continued to face significant challenges. Heavy workloads, inconsistent project management practices, and limited oversight affected the timely delivery of IT initiatives. These challenges were further compounded by the deferred resignation program, which resulted in the loss of experienced personnel and increased responsibilities for the remaining project managers. In response, the CIO developed a more consistent approach for collecting project performance metrics and evaluating whether projects achieved their intended outcomes. Leadership also recognized the need to standardize project management tools and processes to replace the customized approaches that had developed across the organization.

In response, the CIO prioritized rebuilding the federal workforce through an approved hiring action and the TechForce[8] initiative, with plans to hire approximately (b)(5) additional personnel, and OCIO onboarded (b)(5) by the end of FY 2026. HUD also planned to pursue multiple recruitment strategies, including (b)(5) (b)(5) to address immediate staffing needs.

New Metric Gap Challenges

For metric 15, HUD performed vulnerability scans on the network every (b)(5) hours. HUD also began implementing scanning web applications. DHS Binding Operational Directive 23-01, which is criteria that supports this metric, requires vulnerability scanning every 14 days on all IP-addressable assets across all environments. HUD has not yet met this requirement.

[8] https://techforce.gov/

For metric 24, HUD maintained the quality of its security training program during the fiscal year, including the execution and evaluation of its security training strategy and training plan. However, HUD did not demonstrate that its personnel collectively possessed a level of training that showed a reduction in security incidents caused by HUD data users' actions or inactions over time.

For metric 27, HUD did not continuously verify security control implementation across the environment and lacked a trusted real-time view of HUD security posture. HUD continued to rely on manual weekly uploads to the System Security Dashboard, which limited automated, continuous analysis and reduced visibility into current security conditions. HUD continued to work towards implementing a real-time security view through the CDM dashboard as noted earlier in this report. However, HUD did not enroll all systems into the CDM dashboard by the end of FY 2026.

For metric 31, HUD had not fully institutionalized advanced automated response capabilities, such as (b)(5) that continuously stop attacks, misdirect threat actors, and isolate affected systems in real time across the enterprise.

Conclusion

Based on our evaluation, HUD's InfoSec program was determined to be not effective. We assessed HUD at maturity level 3, consistently implemented, based on our evaluation of the 20 core metrics and the 5 supplemental metrics within the 10 domains from the FY 2025 IG FISMA reporting metrics. According to the FY 2025 IG FISMA metrics and OMB guidance, an agency's InfoSec program is effective at maturity level 4, managed and measurable.

HUD had several program improvements including its eICAM development, creating a culture of governance and accountability, and its increased capabilities in monitoring, visibility, and dashboards. The last of these initiatives resulted in an increase in metric maturity in one information security continuous monitoring metric and one incident response metric. The other initiatives also support the overall growth and development of HUD's InfoSec program and future increase in metric maturity.

However, HUD continued to show limitations in addressing longstanding cybersecurity weaknesses including in other areas of its ISCM, data governance, and risk management program. Additionally, HUD faced the challenge of limited technical staffing within the agency. HUD continued to make progress over the past several years in closing FISMA recommendations and should continue to prioritize recommendation closures to improve its cybersecurity posture.

Recommendations

We recommend the Chief Information Officer:

1A. Initiate vulnerability scans at regular intervals for all discoverable assets, including web applications, in accordance with DHS Binding Operational Directive 23-01 (FY 2025 IG FISMA metric 15).

1B. Collect and analyze measurable performance metrics for its security training program to demonstrate that increased workforce skills, knowledge, and abilities are directly reducing security incidents over time caused by user actions or inactions (FY 2025 IG FISMA metric 24).

1C. Implement automated, continuous verification of security controls across all systems. Such as deploying real time compliance monitoring for baseline configurations, patch levels, identity controls, and logging requirements to ensure controls remain consistently implemented and effective throughout the environment (FY 2025 IG FISMA metric 27).

1D. Deploy dynamic or automated reconfiguration capabilities—such as (b)(5) (b)(5) —to quickly isolate or suppress active incidents until HUD can manually respond to the incident (FY 2025 IG FISMA metric 31).

Management Response

OCIO generally agreed with the findings of this report and did not indicate disagreement or request any revisions to recommendations. OCIO offered minor formatting changes throughout the report. OCIO also suggested revised language regarding expired ATOs, the Data Governance Program, and the new metric gap assessments. The OIG evaluated OCIO's management response and made changes to the report where appropriate. Please see Appendix B for the full management response.

OIG Evaluation of Management Response

The OIG acknowledges the continued growth of the data governance program since June 2026. The Data Protection and Privacy domain was rated Managed and Measurable in FY 2026, which speaks to HUD's continued progress towards protecting data. The OIG discussed the depth of the data program as appropriate for the scope of the metrics that support the Data Protection and Privacy domain for the FY 2026 FISMA evaluation. The additional information OCIO provided regarding the program is supplemental and does not impact evaluation results. The OIG adjusted language to ensure the titles within the data governance program were consistent with what OCIO provided.

OCIO asked for clarity on BOD 23-01 requirements in association with IG FISMA metric 15. BOD 23-01 is criteria for metric 15 for the FY 2025 IG FISMA metrics. While it does not impact evaluation results, the OIG adjusted wording in the report to clarify metric 15 and its requirements.

The OIG acknowledges HUD's continued growth in IT visibility through dashboards throughout this report. By the end of FY 2026, HUD did not have all systems enrolled into the CDM dashboard, which will apply automation and support higher maturity for IG FISMA metric 27. Once HUD enrolls all systems to the CDM dashboard, OCIO will have a trusted view of its security posture. While it does not impact evaluation results, the OIG adjusted wording in the report to support HUD's progress towards full implementation.

The OIG acknowledges HUD's plans for automation associated with incident response and IG FISMA metric 31 and commends the department for a well-established plan including ensuring a proper technical foundation and risk considerations. This type of program may support growth in metric maturity once the program is realized within the enterprise.

The OIG's recommendations will remain unresolved and open pending a management decision. We look forward to working with HUD to resolve the recommendations in this report.

Scope and Methodology

We compiled the information necessary to respond to specific FY 2025 IG FISMA reporting metrics for our FY 2026 FISMA independent evaluation. We submitted these responses through the DHS CyberScope application. The submission is provided in appendix C of this report.

As part of FISMA reporting, each agency OIG or an independent external auditor is required to conduct an annual independent evaluation of the effectiveness of the InfoSec program and practices of its respective agency. The scope of our review was department-wide, resulted in conclusions and recommendations made primarily to the OCIO, and covered the period of October 1, 2025, to September 30, 2026.[9]

Fieldwork was based on the FY 2025 IG FISMA Reporting Metrics[10], as CISA instructed independent evaluators to use the FY 2025 IG FISMA metrics for the FY 2026 assessment. We assessed 20 core metrics and 5 supplemental metrics in FY 2026. We selected a sample of information systems from HUD's Inventory of Automated Systems to determine the implementation of its InfoSec program. We also interviewed and collected information from HUD executive leadership with roles related to the InfoSec program and with HUD OCIO personnel responsible for implementing the InfoSec program at the enterprise level.

We then reviewed HUD's progress toward addressing relevant prior recommendations. This supplemental review was designed to address key deficiencies found during prior FISMA evaluations while reducing the repetitiveness of verifying that HUD achieved maturity levels that it reached in prior years. Our approach included the following techniques:

- Interviews with management and system personnel.
- Inspection of documentation related to the implementation of FISMA.
- Data calls to program offices and system points of contact to gather accurate security program data.
- Interviews and demonstrations to gain an understanding of information security, privacy, data protection programs and practices, and system operations.
- Assessments of the implementation and performance of security controls from the NIST SP 800-53, Revision 5 controls.

We evaluated the following levels to accomplish our objectives:

Department level – During this step, we gained an understanding of the FISMA-related policies and guidance that HUD OCIO established. We compared HUD OCIO'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.

[9] This narrative report is based on our FY 2026 CyberScope report, which is provided below in Appendix C. The CyberScope report was issued to HUD on July 30, 2026. However, to the extent the Department provided additional information after the CyberScope report was submitted, we considered it and updated this narrative report accordingly.

[10] FY 2025 IG FISMA Reporting Metrics v2.0 (April 3, 2025). https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf.

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 a program office 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 2026 supplemental metrics across six program office systems, which are listed in figure 3 below.

Table 3 – List of FY 2026 FISMA sample systems

HUD Office	System Name	System Acronym	System Code	System Type	Last FISMA Review
(b)(5)					

Appendices

Appendix A – Prior FISMA Recommendations

HUD OIG has issued 151 recommendations in prior FISMA evaluations since FY 2018. Of the 151 FISMA recommendations, 41 recommendations were still open as of September 30, 2026. In FY 2026, HUD closed 19 recommendations, including 14 FISMA recommendations. As HUD OCIO and the Office of Administration address the remaining open recommendations, HUD will make progress towards improving the maturity of its InfoSec program. Table 4 shows the distribution of these prior open recommendations by the FY that they were issued and the FISMA domain that the recommendation is primarily associated with.

Table 4. Open FISMA Recommendations by Fiscal Year

Domain	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	Domain Total
Cybersecurity Governance									
Cybersecurity supply chain risk management									
Risk and asset management									
Configuration management									
Identity and access management					(b)(5)				
Data protection and privacy									
Security training									
InfoSec continuous monitoring									
Incident response									
Contingency planning									
Fiscal year total	1	0	6	7	3	14	1	9	41

.

Appendix B – Management Response

Docusign Envelope ID: 0D09BE1C-C8C1-8392-8051-227A24F133FB

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
Alexandria, VA. 22314

OFFICE OF THE CHIEF INFORMATION OFFICER

October 28, 2026

MEMORANDUM FOR: Christy Thomas, Director, iTED Division, Office of the Inspector General

FROM: Paul Scott, Assistant Chief Information Officer (CIO)/Business Change and Integration Officer, Office of IT Planning, Policy and Performance (ITPPP), Office of the Chief Information Officer (OCIO)

SUBJECT: HUD Comments on the Draft Evaluation Memorandum: FY 2026 FISMA Evaluation

This memorandum is in response to the Office of the General (OIG) draft FY 2026 FISMA Evaluation. The Office of the Chief Information Officer (OCIO) has reviewed the Draft Report and provided comments.

If you have any questions or require additional information, please contact William Trull, OCIO Audit Liaison Officer, at william.n.trull@hud.gov or Yumiko Ito, Acting Director, Policy and Planning/Audit and Risk Management, at yumiko.ito@hud.gov

Enclosure:

- HUD comments
- HUD Office of General Counsel (OGC) proposed redactions

Paul Scott

Assistant CIO/Business Change and Integration Officer,
Office of IT Planning, Policy and Performance (ITPPP)
Office of the Chief Information Officer
U.S. Department of Housing and Urban Development

For Official Use Only (FOUO)

Docusign Envelope ID: 0D09BE1C-C8C1-8392-8051-227A24F133FB

Draft Evaluation Memorandum: HUD FY 2026 FISMA Evaluation

1. Capitalization - Pg. 4: "FISMA Overview" bulleted list

   HUD Response
   First letter of each bullet is not capitalized, unlike the paragraph above.

   OIG Action
   Capitalize first word of bullets.

2. Correction - Page 7: first paragraph, line 11:
   "Improvement in these areas, along with implementing the corrective actions of the 42 open FISMA recommendations, would address gaps in HUD's FISMA maturity. Refer to Appendix A for a listing of open recommendations by FISMA domain."

   HUD Response
   As of 9/30/2026, there were 41 open FISMA recommendations

   OIG Action
   Please revise to show 41 open FISMA recommendations.

3. Correction – Page 12: first paragraph, line 1:
   "HUD also did not consistently conduct ongoing security control assessments and had more than 58 of its approximately 130 systems operating with expired ATOs, creating significant gaps in continuous monitoring coverage."

   HUD Response
   "HUD also did not consistently conduct ongoing security control assessments for 30 systems. These systems received a conditional ATO letter for one year to ready the system for security assessment."

   OIG Action
   Please replace the sentence with HUD response.

4. Revision – Pages 12-13: Data Program section

   HUD Response
   HUD recommends revising the section to more effectively communicate the ongoing efforts of the CDO program. We recommend changing the paragraphs to the following:

   "In June 2025, the Chief Data Officer (CDO) role transitioned from the Office of Policy Development and Research (PD&R) to the OCIO. Following this realignment, in FY 2026, the CDO re-established a data governance program, which is rounding out its first year in operation with regularly scheduled meetings. The CDO led HUD's enterprise data governance efforts, with an emphasis on establishing department-wide data visibility, strengthening data management practices, and building a foundation for future analytic capabilities. The program

Docusign Envelope ID: 0D09BE1C-C8C1-8392-8051-227A24F133FB

is progressing toward a more structured and coordinated enterprise data governance model, supported by governance bodies and policy development.

HUD established a multi-layered governance model. This model included a Data Governance Board (DGB) comprising all General Deputy Assistant Secretaries as the representative from every program office and a Senior Data Council (SDC) made up of program office data leads. The Data Stewards Community of Practice (DSCoP) was also established and is comprised of program office data stewards and others involved in the data management program. The DGB and SDC are currently working on an updated Enterprise Data Management (EDM) Policy to replace the last one from 2002. The new EDM policy is anchored in HUD's Data Lifecycle Management Framework that the DGB and SDC, which consists of representation from the Privacy and Records offices, reviewed and the CDO adopted in June 2026. The framework consists of six phases and four cross-cutting themes, with 'privacy and security' as one of the cross-cutting themes. The framework is intended to foster compliance by embedding "requirements from federal laws and mandates into data management practices, which reduces the risk of misusing sensitive data and builds public trust that HUD safeguards information while making it appropriately accessible."

The CDO's largest initiative in FY 2026 was the development of the enterprise data catalog. A key challenge for the initiative is HUD's vast systems and interconnectivity of systems, which will require close coordination with OCIO. The vision for the catalog is to support an enterprise data platform, improve data trust and transparency, and enable department-wide analytics. The OIG issued a priority recommendation in the U.S. Department of Housing and Urban Development Personally Identifiable Information (PII) Risk Management in a Zero Trust Environment (2023-OE-0007) Evaluation Report in 2024, recommending the Agency to develop an enterprise data inventory/catalog HUD's PII. Several of HUD's systems have been onboarded into the test environment and the team continues to work with HUD system owners to onboard the remaining known HUD systems. The CDO also received its security authorization, which will allow it to move the Enterprise Data Catalog into the production environment. Data Stewards will capture and validate metadata for these systems in the production environment. The CDO Office has developed the Data Catalog Quick Reference Guide to guide the Data Stewards in this process and includes directions for Data Stewards to note any type of Controlled Unclassified Information (CUI) the system may contain, in accordance with HUD's Controlled Unclassified Information Policy.[1] This guidance will be reinforced through workshops and training sessions with the DSCoP, which has over 70 members and has been meeting monthly since May 2026.

HUD reported that resources, such as funding and personnel for the data governance program are limited. The CDO's budget resides in the Office of PD&R, yet the role of the CDO resides within OCIO. Funding only covers contractor support through early February 2027. The CDO is reliant on contractor support to finish the data catalog. Lastly, there are only approximately 1.5 full-time government employees dedicated to data governance operations. The success of HUD's enterprise data governance program also depends heavily on active participation from

[1] CUI policy can be found here: https://www.hud.gov/sites/dfiles/OCHCO/documents/22001c17ADMH.pdf

program offices. While some offices demonstrate strong engagement, others are still adapting to governance expectations, emphasizing the need for cultural change and a shift away from siloed data practices. Without appropriate resources, HUD cannot improve its data governance program. This limits HUD's ability to mature in areas of governance, risk, access, and data protection and privacy, which are reliant on the ability to follow data throughout its environment."

OIG Action
Please replace the section with HUD responses.

5. Typo - Page 13: Risk Management Challenges paragraph, line 8:
"While the program faced challenges in FY 2026, the OIG did not issue additional risk and asset management recommendation1s, as the department should address the 14 current open recommendations to mature this domain."
HUD Response
Correct typo to "recommendations"

OIG Action
Please correct typo.

6. Correction - Page 14: Paragraph 4, line 2:
"…although none were yet onboarded by the end of FY 2026"

HUD Response
There was a total of 52 personnel that were onboarded for OCIO by the end of FY 2026.

OIG Action
Please correctly show OCIO onboarded 52 personnel before the end of FY 2026.

7. Revision – Page 14: New Metric Gap Challenges paragraph 1
"For metric 15, HUD performed vulnerability scans on the network every 72 hours. HUD also began implementing scanning web applications. Because HUD had not fully implemented this scanning program, it does not yet meet the requirements of DHS Binding Operational Directive 23-01, which requires vulnerability scanning every 14 days on all IP-addressable assets across all environments."

HUD Response
HUD recommends revising or clarifying this finding to accurately reflect the scope of DHS Binding Operational Directive (BOD) 23-01 versus the CIO FISMA Metrics. While the draft report states that HUD's scanning program "does not yet meet the requirements of DHS BOD 23-01" due to incomplete web application scanning, this conflates two distinct compliance frameworks:

- DHS BOD 23-01 Scope: This directive specifically governs basic IP-addressable assets (such as network infrastructure, hosts, and standard vulnerability enumeration). It does not focus on or mandate web application scanning. HUD fully complies with

Docusign Envelope ID: 0D09BE1C-C8C1-8392-8051-227A24F133FB

BOD 23-01 by performing comprehensive network vulnerability scans every 72 hours, easily exceeding the directive's 14-day requirement.

- FISMA Metrics Scope: Web application scanning is separately evaluated under the Environment Enumeration and Vulnerability Management controls of the active FY 2025 / FY 2026 CIO FISMA Metrics (which also carries a 14-day scanning requirement).
- HUD's network infrastructure scanning is fully operational and compliant with BOD 23-01

OIG Action

Please further clarify by decoupling the web application scanning assessment from the BOD 23-01 compliance conclusion and evaluate it strictly under the appropriate FISMA metric.

8. Revision - Page 15: Paragraph 1
"For metric 27, HUD did not continuously verify security control implementation across the environment and lacked a trusted real-time view of HUD security posture. HUD continued to rely on manual weekly uploads to the System Security Dashboard, which limited automated, continuous analysis and reduced visibility into current security conditions."

HUD Response

HUD requests the revision of this finding, as the factual premise regarding manual weekly uploads is entirely incorrect.
The draft report states that HUD relies on "manual weekly uploads to the System Security Dashboard," which is factually inaccurate. HUD's Continuous Diagnostics and Mitigation (CDM) data architecture is fully automated and functions as follows:

- Automated Scanning & Collection: HUD utilizes Layer A tools that execute automated, continuous security control scans across the environment without human intervention.
- Automated Aggregation & Feeds: The data collected by these tools is automatically aggregated and fed directly into the CDM Dashboard.
- Real-Time Data Flow: Because this pipeline is fully programmatic, there are no manual processes, weekly file uploads, or human interventions required to populate the dashboard.
- HUD has a trusted, automated data pipeline that continuously verifies security control implementation.

OIG Action

Please verify the automated data exchange logs between HUD's Layer A tools and the CDM Dashboard to correct this finding in the final report.

9. Current Language - Page 15: Paragraph 2
"For metric 31, HUD had not fully institutionalized advanced automated response capabilities, such as automated firewall rule modifications, router reconfigurations, or dynamic access control adjustments that continuously stop attacks, misdirect threat actors, and isolate affected systems in real time across the enterprise."

Docusign Envelope ID: 0D09BE1C-C8C1-8392-8051-227A24F133FB

HUD Response
HUD acknowledges the recommendation for metric 31 and is actively evaluating its automated response capabilities through the deployment of tools like Sumo Logic Cloud SOAR (Security Orchestration, Automation, and Response). While fully autonomous, real-time enterprise-wide reconfigurations (such as automated firewall or router modifications) require careful risk management to prevent accidental operational disruptions, HUD is laying the technical foundation to automate critical incident workflows.

HUD requests that the finding be updated to reflect this ongoing progress:

- HUD may use Sumo Logic Cloud SOAR to automate incident triage, investigation, and containment workflows. This would significantly reduce response times and streamlines how the Security Operations Center (SOC) isolates potential threats.
- Risk-Managed Automation: HUD is actively evaluating safe, phased implementations of advanced orchestration capabilities, including dynamic access control adjustments - ensuring they are thoroughly tested before full enterprise deployment.
- Next Steps: The SOC is continuously maturing its SOAR playbooks to expand automated remediation while maintaining necessary operational safeguards.

OIG Action
Please update the language to acknowledge the current implementation efforts rather than characterizing the capability as entirely absent.

10. Typo – Page 17: "Scope and Methodology" bulleted list

HUD Response
First letter of each bullet is not capitalized.

OIG Action
Please capitalize first word of bullets.

11. Correction - Page 19: First paragraph, first line:
"HUD OIG has issued 151 recommendations in prior FISMA evaluations since FY 2018. Of the 151 FISMA recommendations, 42 recommendations were still open as of September 30, 2026."

HUD Response
As of 9/30/2026, there were 41 open FISMA recommendations

OIG Action
Please revise to show 41 open FISMA recommendations.

12. Correction - Page 19: Table 4: FY 2025 10 open FISMA recommendations

HUD Response
There were 13 recommendations from the FY 2025 FISMA evaluation. OCIO closed the four below in FY 2026.

Docusign Envelope ID: 0D09BE1C-C8C1-8392-8051-227A24F133FB

- 2026-OE-0001-1I
- 2026-OE-0001-1J
- 2026-OE-0001-1K
- 2026-OE-0001-1L

OIG Action

9 FISMA recommendations remain open from FY 2025.

Appendix C – FY 2026 HUD OIG CyberScope Submission

The inserted document below contains HUD OIG's responses for the FY 2026 FISMA evaluation using the FY 2025 IG FISMA metrics that were established by OMB. The document below was submitted to the DHS CyberScope application on July 30, 2026.

The subsequent section of the report is not being publicly released due to concerns about the risk of circumvention of the law: Appendix C, FY 2026 HUD OIG CyberScope submission.

Appendix D – FISMA Metric Trends

Since FY 2022, we assessed the 20 core metrics, so they can be used to measure HUD's progress in improving its InfoSec maturity over time. Table 5 shows the core metric maturity trends since FY 2022.

Table 5. Core metric maturity trends since FY 2022

Metric #	FY 2022 Rating	FY 2023 Rating	FY 2024 Rating	FY 2025 Rating	FY 2026 Rating
5	Ad hoc	Ad hoc	Defined	Consistently implemented	Consistently implemented
7	Defined	Defined	Defined	Consistently implemented	Consistently implemented
8	Consistently implemented	Defined	Managed and measurable	Consistently implemented	Consistently implemented
9	Consistently implemented	Defined	Consistently implemented	Consistently implemented	Consistently implemented
11	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented
12	Defined	Defined	Defined	Defined	Defined
14	Defined	Defined	Consistently implemented	Consistently implemented	Consistently implemented
15	Defined	Defined	Defined	Consistently implemented	Consistently implemented
17	Defined	Ad hoc	Defined	Defined	Defined
18	Defined	Ad hoc	Defined	Defined	Defined
19	Defined	Defined	Defined	Consistently implemented	Consistently implemented
21	Defined	Defined	Consistently implemented	Consistently implemented	Consistently implemented
22	Defined	Consistently implemented	Managed and measurable	Managed and measurable	Managed and measurable
24	Consistently implemented	Consistently implemented	Managed and measurable	Managed and measurable	Managed and measurable
26	Defined	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented
28	Defined	Consistently implemented	Consistently implemented	Consistently implemented	Defined
30	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented	Managed and measurable
31	Consistently implemented	Consistently implemented	Managed and measurable	Managed and measurable	Managed and measurable
33	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented
34	Defined	Consistently implemented	Managed and measurable	Managed and measurable	Managed and measurable