




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

HUD Fiscal Year (FY) 2025 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation

2026-OE-0001

December 18, 2025



The following record is a HUD OIG document. The redactions applied to four new recommendations found in the *Conclusion and Recommendations* section and the redactions applied in the *List of Open FISMA Recommendations from Prior Evaluations* found in Appendix B were asserted by HUD OIG. However, all other 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

FY 2025 FISMA EVALUATION | 2026-OE-0001

Why We Did This Evaluation

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.

Results of Evaluation

The Office of Management and Budget (OMB) issued the fiscal year (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. HUD continued to show incremental progress in improving its InfoSec program in FY 2025. HUD maintained an overall rating of maturity level 3, consistently implemented. OMB guidance states that maturity level 4, managed and measurable, is an effective level of maturity.

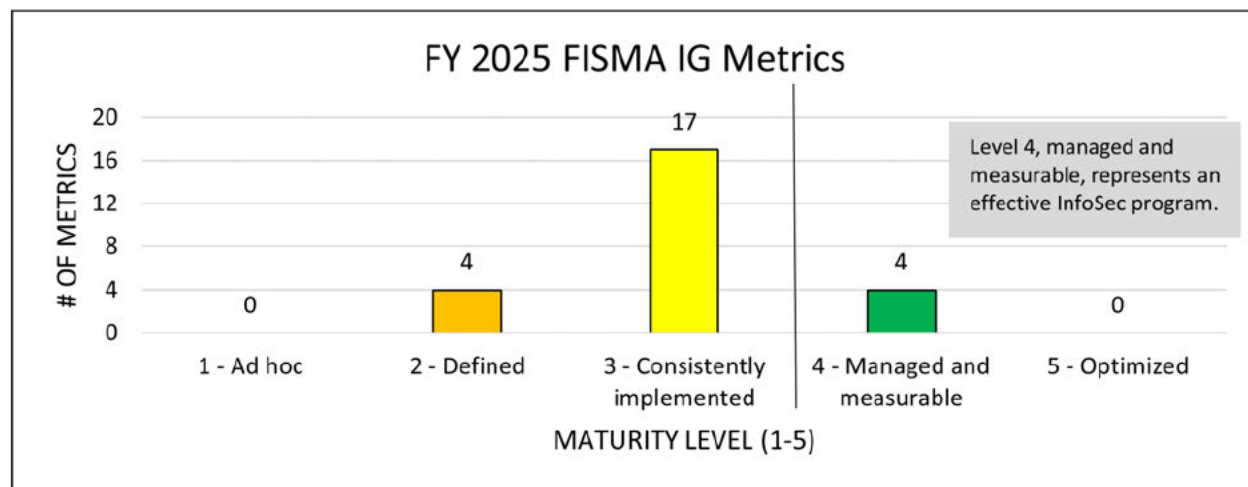
Although HUD has not yet achieved an effective level of maturity for its InfoSec program, we continued to see HUD demonstrate progress in FY 2025. HUD increased in maturity in 4 metrics, 1 domain, and 1 function. HUD also achieved maturity level 3, consistently implemented, in 4 of the 5 supplemental metrics that were first assessed this year. Key areas where HUD improved included continuing to use its Continuous Diagnostics and Monitoring (CDM) dashboard and maturing in how the CDM dashboard was used; finalizing and implementing its Cybersecurity Supply Chain Risk Management (C-SCRM) policies and procedures, which allowed HUD to have better awareness on the risks of its IT supply chain; providing contractors with government-furnished equipment (GFE) to have better control over the IT assets its contractors are using instead of relying on their non-GFE equipment; and adapting to new cybersecurity requirements that were identified in the supplemental metrics.

However, we identified that there was a temporary suspension of the InfoSec Continuous Monitoring (ISCM) program to complete a transition to new security controls. HUD reported that the ISCM program should resume by (b) (5), and the transition to new security controls should be completed by (b) (5). This suspension resulted in a decrease in maturity in metric 8. If HUD restarts its ISCM program as planned, it should resolve the decrease in maturity and potentially improve the maturity of other metrics that require an implemented ISCM program to reach maturity level 4, managed and measurable.

We also found that HUD did not finish developing an integration that would provide timely and updated security information to HUD stakeholders to guide their decision making. HUD identified and was still working to implement a (b) (5), which would support several InfoSec program needs. Poor coordination between HUD's enterprise-wide business impact analysis and other contingency planning documents resulted in two lists of the priority of recovering systems in the event of an incident that were not consistent with each other. HUD also had only just started developing a (b) (5) across HUD and had not implemented strong multi-factor authentication (MFA) across the agency.

We assessed HUD’s maturity across 25 metrics. HUD scored 3.13 in the 20 core metrics that we have assessed every year since FY 2022, and it scored 2.67 in the 5 supplemental metrics that were first assessed in FY 2025. Figure 1, below, shows the distribution of HUD’s metric maturity levels. HUD had no metrics assessed at the lowest maturity level (maturity level 1, ad hoc), which was an improvement from last year. HUD also improved by having only 4 metrics at maturity level 2, defined, down from 8 metrics assessed at that level last year. This indicated that the InfoSec program was moving toward the implementation level, a necessary step to achieving an effective InfoSec program at maturity level 4, managed and measurable.

Figure 1 – HUD’s distribution of metric maturity scores



Recommendations

This report contains 13 new recommendations to improve HUD’s InfoSec program to achieve maturity level 4, managed and measurable. We target our recommendations to guide HUD to the next maturity level and to address any identified weaknesses at the lower maturity levels that still exist. In addition, we focus first on making recommendations to bring all metrics to maturity level 4, managed and measurable, which represents an effective level of maturity. A list of HUD’s open recommendations is provided in Appendix B.

Table of Contents

Introduction	1
Objectives.....	1
Background.....	1
Results of Review	4
HUD Did Not Have an Effective InfoSec Program in FY 2025.....	4
Spotlight on Key Initiatives	5
Program Improvement Needs	10
Conclusion and Recommendations	15
Scope, Methodology, and Limitations	19
Scope.....	19
Methodology.....	19
Sample System Descriptions from SSPs and HUD’s IAS	20
Reporting.....	22
Limitations.....	22
Appendixes	23
Appendix A – Management Response.....	23
Appendix B – Prior FISMA Recommendations.....	28
Appendix C – Abbreviations.....	35
Appendix D – FY 2025 HUD OIG CyberScope Submission.....	37
Appendix E – HUD FISMA Metric Trends	38

Introduction

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:

- 1A. Performing the annual independent evaluation of the effectiveness of HUD's InfoSec program and practices as required by FISMA.¹
- 1B. 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.
- 1C. 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.²
- 1D. Preparing responses for each applicable Office of Management and Budget (OMB)/DHS CyberScope IG FISMA questions, with the support and conclusions documented for each response.

BACKGROUND

FISMA requires all IGs to assess the effectiveness of the InfoSec program of their 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.² OMB also publishes guidance to IGs and Federal agencies on how to assess the IG FISMA metrics, required reporting timelines, and InfoSec priority focus areas of the administration.³ 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.

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.

³ M-25-04, FY 2025 Guidance on Federal Information Security and Privacy Management Requirements (January 15, 2024). <https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf>.

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.
- 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.

FISMA also requires each agency IG to conduct an annual independent evaluation to determine the effectiveness of the InfoSec program and practices of its parent agency. Additionally, agency OCIOs must submit Chief Information Officer (CIO) metrics quarterly to OMB. The CIO metrics are also organized around NIST security guidelines. In accordance with OMB guidance in OMB Memorandum (M)-25-04, the FY 2025 quarterly CIO metric responses should report the implementation of NIST standards and cybersecurity-related initiatives, including those related to FY 2021 Executive Order (EO) 14028, “Improving the Nation’s Cybersecurity” and those related to the new Govern function of the NIST Cybersecurity Framework (CSF) 2.0.⁴

IG FISMA Metrics

OMB issued the final FY 2025 IG FISMA metrics on April 3, 2025, which included a total of 25 metrics for IGs to assess. The metrics were divided into 2 categories, as follows:

- 5 new supplemental metrics, which have never previously been assessed by OIGs; and
- 20 core metrics, which have been assessed by OIGs annually since FY 2022.

OMB selected the 20 core metrics in FY 2022 to represent a combination of high-impact security processes and essential functions necessary to determine HUD’s overall InfoSec program effectiveness. The core metrics were primarily chosen to align with EO 14028.⁴ 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 E.

⁴ EO 14028, “Improving the Nation’s Cybersecurity” (May 12, 2021). <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>. NIST CSF 2.0. <https://www.nist.gov/cyberframework>.

Metric and Domain Alignment to the NIST CSF 2.0

In FY 2025, the IG FISMA metrics were re-aligned from the previous NIST CSF 1.1 to NIST CSF 2.0. The primary change in the new NIST CSF 2.0 is the creation of a new Govern function which includes a new Cybersecurity Governance domain that consists of 3 new supplemental metrics. In addition, Supply Chain Risk Management (SCRM) was renamed to Cybersecurity SCRM (C-SCRM) and moved into the new Govern function. Figure 1 below shows how the 6 NIST CSF 2.0 functions of Govern, Identify, Protect, Detect, Respond, and Recover are aligned to the 10 FISMA domains.

Figure 2 – NIST CSF 2.0 function and FISMA domain alignment

NIST CSF 2.0 Function	Sample
Govern	<ul style="list-style-type: none"> • Cybersecurity Governance • Cybersecurity Supply Chain Risk Management
Identify	<ul style="list-style-type: none"> • Risk and Asset Management
Protect	<ul style="list-style-type: none"> • Configuration Management • Identity and Access Management • Data Protection and Privacy • Security Training
Detect	<ul style="list-style-type: none"> • InfoSec Continuous Monitoring
Respond	<ul style="list-style-type: none"> • Incident Response
Recover	<ul style="list-style-type: none"> • Contingency Planning

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 has 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 3, below, shows an overview of the FISMA maturity model.

Figure 3 – FISMA maturity model levels



Results of Review

HUD DID NOT HAVE AN EFFECTIVE INFOSEC PROGRAM IN FY 2025

In FY 2025, we assessed HUD at maturity level 3, consistently implemented, for its overall InfoSec program. HUD has made incremental progress across its InfoSec program and should continue to take steps to improve the security of its IT systems and assets, which will lead to an increase in its FISMA maturity level.

As noted in the introduction, OMB selected 20 core metrics that represented high-impact security processes and essential functions in FY 2022. We have assessed the core metrics every year since FY 2022, and HUD's trend of increasing scores continued in FY 2025. This demonstrates the progress HUD has made in maturing its InfoSec program over that time. Figure 4 below shows HUD's increase in core metric maturity, which improved every year from FY 2022 to FY 2025.

Figure 4 – HUD's progress in core metric maturity since FY 2022

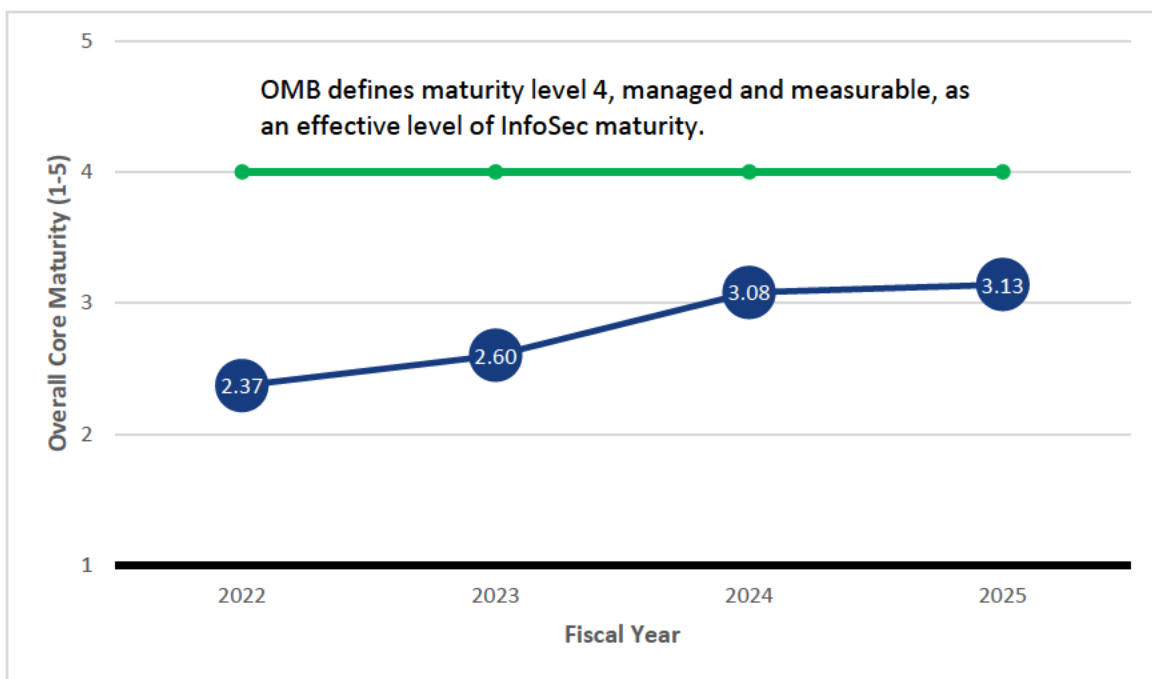


Figure 5 below summarizes the number of metrics assessed at each maturity level by FISMA domain and the assessed ratings of each domain and metric.⁵

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

Figure 5 – Summary of FISMA metrics by function and domain

NIST CSF 2.0 Function	FISMA domain	Defined	Consistently implemented	Managed and measurable	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	0	3	0	Consistently implemented
Respond	Incident response	0	1	1	Managed and measurable
Recover	Contingency planning	0	1	1	Managed and measurable
Overall		4	17	4	Consistently implemented

SPOTLIGHT ON KEY INITIATIVES

Below showcases areas where HUD has made progress in improving its InfoSec program in FY 2025.

Continuous Diagnostics and Mitigation (CDM) Dashboard

HUD used its CDM dashboard to maintain awareness of its systems, hardware assets, and software assets and to provide an accurate inventory of its InfoSec assets. Maintaining an accurate inventory of assets is foundational to the overall cybersecurity program to properly secure those assets, identify potential threats to information systems, and respond to threats if an incident occurs. HUD’s CDM dashboard provided this awareness of system and IT assets.

In addition, HUD’s CDM dashboard tracked identified vulnerabilities and misconfigurations. HUD used this information to remediate issues discovered through its scanning programs. HUD aligned its

vulnerability and configuration scanning timelines in FY 2025 to meet DHS requirements⁶ except for web applications, which were still not covered by a timely scanning program.

HUD used the CDM dashboard to ensure its assets remained up to date on patches so that they were secured from known vulnerabilities. HUD resolved discrepancies in its reported inventory and aligned most scanning timelines, as noted above. The next steps that HUD should take to improve its awareness of InfoSec assets and ensure their security are:

1. Addressing the gap in scanning timelines for web applications to meet DHS standards; and
2. Resuming the ISCM program (discussed below in Program Improvement Needs) to have timely updates to the information in its CDM dashboard.

HUD's initiatives in this area led to an increase in maturity score for IG FISMA metrics 7 and 15. Metric 7 was related to HUD's inventory of its information systems, and the CDM dashboard provided consistent information on HUD's information systems. Metric 7 increased to maturity level 3, consistently implemented. Metric 15 was related to HUD's scanning and patching program for security vulnerabilities. Although HUD does need to address web applications, as noted above, HUD implemented the remainder of the vulnerability scanning and remediation program in a consistent manner that led to an increase to maturity level 3 for this metric.

Transition to Government-Furnished Equipment (GFE) for Contractors

Historically, OCIO faced challenges ensuring that contractor laptops met HUD's security requirements. Because HUD's contractors were using their own devices, HUD did not have direct visibility into the security posture of these devices. For example, contractor laptops would be subject to the contractor's own policies for security updates instead of HUD's policy. HUD took mitigating steps in prior years, such as requiring minimum security requirement agreements with contractors. For example, OCIO could detect unpatched laptops, but they could not directly patch the laptops, because they did not own or manage the devices.

In FY 2025, HUD notified contractors of a change in policy that the contractors would be required to obtain and use HUD GFE laptops to access most HUD systems.⁷ This transition to GFE greatly reduced the risks associated with the contractor laptops. In addition, it reduced HUD's threat surface and risk exposure by unifying the devices that access HUD's systems to those under OCIO's management. OCIO's ability to provide GFE devices to contractors allowed the implementation of this program that reduced HUD's IT risk from non-GFE devices.

⁶ DHS Binding Operational Directives (BOD) are requirements that HUD must comply with as a Federal agency. DHS BODs 19-02, 22-01, and 23-01 contain requirements that IT assets are scanned every 14 days, critical vulnerabilities are remediated within 15 days, and high vulnerabilities are remediated within 30 days. The intent of the DHS requirements is to ensure that the most critical vulnerabilities are detected and remediated quickly before threat actors can use them to attack the agency.

⁷ HUD did not mandate the use of GFE to access cloud-based systems. However, due to the nature of cloud-based systems, this is not as significant of a threat. Cloud-based systems run on hardware owned and operated by the cloud service provider. Access to cloud-based systems is generally through an Internet portal. Therefore, the risk of attack attributable to contractor laptops vs. GFE is reduced, though not eliminated.

However, HUD still permitted non-GFE devices in some other contexts, such as the option to use personal phones, known as a bring-your-own-device (BYOD) program. BYOD phones used at HUD were subject to a mobile device management (MDM) platform that allowed OCIO to manage those devices to a limited extent so that OCIO could enforce minimum security requirements. HUD's MDM platform mitigated the risk of BYOD phones being unpatched.

Because HUD still permits some non-GFE devices, such as BYOD phones, the Rules of Behavior (ROB) still needed to cover the use of these devices on the HUD network. HUD had a ROB that stated that BYOD devices were required to comply with cybersecurity requirements and could be analyzed in the event of a security incident. However, HUD has an open recommendation to develop procedures for how it would get the BYOD device from a user for analysis (2023-OE-0001-19).⁸

HUD's transition to GFE equipment for contractors supported increased maturity scores in IG FISMA metrics 15 and 19. Metric 15, as noted above, relates to the security vulnerability management program, and bringing the IT equipment under OCIO control allowed for better management of security vulnerabilities. Metric 19 required, in part, that HUD establish user accounts in accordance with the principle of least privilege by ensuring that each user only has access to and authority in information systems that are necessary to perform their job role. The transition again gives OCIO better management and control over the user accounts to ensure that this principle was followed. Metrics 15 and 19 improved to maturity level 3, consistently implemented in FY 2025.

Improved Policies and Procedures

Effective implementation of cybersecurity tasks depends on a strong foundation of strong policies and procedures. In FY 2025, HUD continued to improve the effectiveness of its InfoSec policies and procedures to support stronger IT governance and compliance. Key areas where HUD updated its InfoSec policies and procedures in FY 2025 included clarification on inventorying web applications; finalizing and implementing C-SCRM policies and procedures; and updating the enterprise cyber-role analysis (ECRA).

First, HUD updated its Inventory of Automated Systems (IAS) user guide to clarify how it inventoried web applications. IAS served as HUD's official inventory of IT systems. However, in previous years, HUD had web applications that were not included in IAS. HUD updated its user guide to explain that web applications would be inventoried in a (b) (5). IAS and the WASP site now serve as a combined IT systems inventory, with web applications inventoried in the WASP site and all other systems inventoried in IAS. This update addressed an open recommendation from the FY 2024 FISMA evaluation to clarify the inventory requirements for all systems (2024-OE-0002-01).⁹ This revision and clarification of the IAS guide supported the increase in maturity for IG FISMA metric 7, related to having an accurate inventory of information systems, to maturity level 3, consistently implemented.

⁸ 2023-OE-0001-19, HUD FY 2023 FISMA Evaluation Report, Recommendation 19 (January 29, 2024).

<https://www.hudoig.gov/reports-publications/report/hud-fy-2023-federal-information-security-modernization-act-fisma>.

⁹ 2024-OE-0002-01, HUD FY 2024 FISMA Evaluation Report, Recommendation 1 (October 29, 2024).

<https://www.hudoig.gov/reports-publications/report/hud-fy-2024-federal-information-security-modernization-act-fisma>.

Second, HUD finalized its C-SCRM policies and procedures to ensure that products, system components, and services met its cybersecurity and supply chain requirements. As part of the implementation of the C-SCRM procedures, half of the systems reviewed updated their system security plans (SSP) to reflect the use of the new C-SCRM controls. The remaining systems reviewed did not update their SSPs by the end of the evaluation period but took other C-SCRM-related actions such as completing cybersecurity risk assessments for support contractors and obtaining C-SCRM attestation letters from vendors to confirm they followed secure software development practices.

In addition, HUD's C-SCRM program team also conducted risk assessments on vendors to evaluate potential supply chain threats. HUD maintained a risk register to track supply chain risks and added the vendor assessment results to this register for ongoing monitoring. By formalizing and applying C-SCRM practices, HUD identified, assessed, and mitigated risks associated with third-party vendors and suppliers. These improvements enhanced HUD's resilience against supply chain disruptions and potential cybersecurity threats. In today's threat environment, HUD must not only ensure that it has an effective cybersecurity program, but it must be aware of the risks from its vendors and suppliers too. The implementation of HUD's C-SCRM program led to an increase in maturity in IG FISMA metric 5 to maturity level 3, consistently implemented. Metric 5 was related to how HUD implemented its C-SCRM program.

Finally, HUD updated its ECRA in FY 2025. The ECRA assigned responsibility for reviewing and updating cybersecurity training materials to personnel in the cybersecurity workforce management, cybersecurity curriculum development, and cybersecurity instruction roles. It also provided a structured way for HUD to evaluate its current training programs, identify ineffective areas, and understand cybersecurity skill needs across HUD. HUD normally updates the ECRA at the end of each fiscal year and then uses those results to update the security training plan for the following fiscal year. In FY 2025, HUD personnel updated the ECRA, which they planned to use to make changes in FY 2026, and they also made changes to the FY 2025 security training plan based on the results from the FY 2024 ECRA. By having an updated ECRA, HUD was able to refresh existing training content to improve its effectiveness; identify areas that need new training; and align personnel's security training requirements with their roles. Security threats are constantly evolving, so having up-to-date training materials and a timely view of any cybersecurity skills gap is an important part of ensuring that HUD's personnel can effectively support the InfoSec program. HUD's annual review of the ECRA to determine what improvements were needed for its security training program supported its continued assessment of maturity level 4, managed and measurable in IG FISMA metric 24, which was related to assessing the knowledge and skills of HUD personnel.

Implementation of New Supplemental FISMA Metric Requirements

In FY 2025, OMB directed OIGs to assess five new supplemental metrics. We discuss HUD's progress in responding to the new supplemental metric requirements in this section. HUD achieved maturity level 2, defined, in metric 10, related to establishing a data inventory, which is discussed in more details below as a Program Improvement Need. Except for metric 10, however, HUD demonstrated its ability to respond to evolving InfoSec requirements by achieving higher maturity levels in the remaining four supplemental metrics.

Cybersecurity Governance

Three of the five supplemental metrics were in the new Cybersecurity Governance domain. We generally found that HUD was implementing the metric requirements through other InfoSec programs. However, HUD will need to formalize some of its processes for handling its governance programs so that the roles and responsibilities are clear to stakeholders and continue to be implemented over time. The new governance metrics covered cybersecurity risk management strategy, cybersecurity resources and performance monitoring of personnel, and cybersecurity profiles.

Cybersecurity Risk Management Strategy

The first supplemental metric we discuss in the Cybersecurity Governance domain was related to how HUD used a cybersecurity risk management strategy that included priorities, constraints, assumptions, risk tolerance, and risk appetite. HUD's OCIO and ERM program coordinated cybersecurity risks as part of HUD's overall risk strategy. OCIO was the primary lead on cybersecurity risks, but when significant risks were identified, they were communicated to the ERM team. In addition, when other program offices or the ERM team identified risks that included cybersecurity programs, those risks were assigned to OCIO for monitoring. This coordination ensured that HUD's overall risk strategy considered cybersecurity risks as a key component and that HUD's InfoSec program was in alignment with the overall risk strategy. HUD achieved maturity level 3, consistently implemented, in this IG FISMA metric.

Cybersecurity Resources and Personnel Performance Monitoring

The second supplemental metric in the Cybersecurity Governance domain was related to how HUD allocated resources in accordance with its risk strategy and how personnel had their performance assessed and were held accountable. We found that cybersecurity personnel across HUD were generally performing their duties as expected. HUD faces some challenges in monitoring roles and responsibilities across the organization because not all cybersecurity roles are within OCIO. Some program office staff also served in cybersecurity-related positions, such as Information System Security Officers. HUD achieved maturity level 3, consistently implemented, in this IG FISMA metric.

Cybersecurity Profiles

The final new governance metric was related to developing and implementing cybersecurity profiles. NIST provided a template document for creating an organizational cybersecurity profile that HUD may choose to leverage. However, cybersecurity profiles do not have to be in a specific format. Rather, the purpose of a cybersecurity profile for HUD is to identify the state of its InfoSec program as it is today and as HUD plans for it to be in the future. The cybersecurity profile can then serve as a roadmap from the current state to the desired target state. HUD had several documents including multiple strategies and plans that addressed part of the InfoSec program. For example, HUD's ECRA, discussed previously, provides an annual review of the security training program. An effective organizational cybersecurity profile would consolidate high-level information across the various parts of HUD's InfoSec program into a single place for stakeholders to see the overall progress towards achieving HUD's cybersecurity goals. HUD could also leverage further cybersecurity profiles at lower levels if it chooses to do so, such as for individual program offices or systems. HUD achieved maturity level 3, consistently implemented, in this IG FISMA metric.

ISCM

Measuring the Security Posture of IT Assets

The final new metric that was assessed in FY 2025 was in the ISCM domain, and it was related to monitoring the security posture of HUD's IT assets. HUD's security operations center (SOC) provided effective monitoring of HUD's IT assets, including addressing a priority recommendation to monitor network traffic that is discussed below. The SOC also investigated incidents and isolated devices that did not comply with HUD's security requirements, which reduced the risks of vulnerabilities being exploited in the first place. Further, if a threat actor had exploited a vulnerability, then isolating the affected devices reduced the risk of an attacker being able to spread throughout the network and compromise other devices. HUD achieved maturity level 3, consistently implemented, in this IG FISMA metric.

PROGRAM IMPROVEMENT NEEDS

Below we discuss areas where HUD faced challenges in improving its InfoSec program that we observed in FY 2025.

HUD's Delayed ISCM Transition

In April 2025, HUD reported that it encountered challenges in completing its planned transition from NIST Special Publication (SP) 800-53, Rev. 4 security controls to Rev. 5 security controls. As part of the transition, HUD personnel reported that it had suspended ISCM assessments due to staffing changes and because of the potential for inconsistent data reporting with some systems still under the Rev. 4 controls and other systems that had already transitioned to Rev. 5 controls. The NIST SP 800-53 Rev. 5 controls align to the NIST CSF 2.0 framework described in the introduction above. Agencies were required to transition to the Rev. 5 controls by September 2021 to ensure that system security controls remained up to date in an ever-changing threat environment.

HUD personnel stated that they expected to complete the transition to Rev. 5 controls by (b) (5), which was about (b) (5) later than they had previously reported in our FY 2024 evaluation. This delay increased the length of time that systems used the outdated Rev. 4 controls.¹⁰ HUD intended to resume regular ISCM assessments by January 2026 with most systems transitioned to the new Rev. 5 controls by that time.

HUD took steps to mitigate the delay in conducting ISCM assessments. For example, system stakeholders that we interviewed reported that (b) (5). As HUD resumes its ISCM assessments, it will have more timely information on the security posture of its IT systems and assets that will increase the effectiveness of the CDM dashboard. In the rapidly changing threat environment that agencies face, untimely information may have limited value in ensuring the security of HUD's IT systems. Restarting the ISCM program would improve maturity in metrics 26 and 28 in the ISCM domain and would support the requirements of multiple metrics in other domains that require integration with the ISCM program at higher maturity levels.

¹⁰ An analysis of the changes from NIST SP 800-53 Rev. 4 to Rev. 5 controls that is provided by NIST identifies 698 substantive changes to the security controls. "Analysis of updates between 800-53 Rev. 5 and Rev. 4, by MITRE Corp for ODNI." <https://csrc.nist.gov/files/pubs/sp/800/53/r5/upd1/final/docs/sp800-53r4-to-r5-comparison-workbook.xlsx>.

Continued InfoSec Weaknesses

Although HUD showed improvement in some areas noted above in the key initiatives section, there were other areas of its InfoSec program that continued to have weaknesses. First, HUD continued its transition to multi-factor authentication (MFA) across the agency, to address recommendations issued in FY 2020. Second, HUD still needed to address user logging. Third, HUD did not meet Trusted Internet Connection (TIC) 3.0 requirements. Finally, HUD did not implement an automated governance, risk, and compliance (GRC) tool.

MFA

HUD has still not fully transitioned to MFA. HUD established a new enterprise identity and access management (EIDAM) program management office (PMO) this fiscal year to help consolidate efforts to transition to MFA across the agency. The EIDAM PMO planned to implement MFA across the agency by FY 2027. HUD has had multiple MFA strategies in the past, but HUD replaced each strategy as personnel identified challenges during MFA implementation. The EIDAM PMO planned to develop a new MFA strategy by the end of FY 2025. HUD originally received \$14.8 million in funding from the Technology Modernization Fund (TMF) to implement a pilot implementation of MFA to 15 systems using FHA Connection beginning in FY 2023. HUD also deployed phishing-resistant MFA to 9 systems under FHA Connection as of FY 2025. HUD was awarded additional TMF funding to continue expanding MFA across HUD's information systems at the beginning of FY 2025. HUD has received 90% of the \$19.8 million in additional TMF funding for this new award as of September 2025. HUD should use the TMF funds to ensure secure access through MFA for both general users and users with elevated access to all HUD systems. HUD has two open priority recommendations to implement MFA for both nonprivileged users (2020-OE-0001-15) and to implement MFA for privileged users (2020-OE-0001-16).¹¹ Implementing MFA would improve HUD's maturity in metrics 17 and 18.

User Logging

HUD was still in the process of implementing user logging, even though OMB M-21-31 required HUD to meet the first level of user logging by September 2022. OMB M-21-31 established a three-tier system of logging requirements, beginning with level event logging (EL) 1, basic. HUD did not achieve EL1 logging in FY 2025. User logging is a valuable resource when analyzing a security incident because it serves as a record of what actions were taken and by whom. In addition, logs can be used proactively to identify certain security events as they occur. For example, HUD user activities outside of normal business hours in their time zone might indicate a breach by an attacker in a different time zone. HUD has an open recommendation to define a plan to implement the required user logging levels (2023-OE-0001-17).¹² Achieving EL1 logging and further implementing EL2 logging would improve HUD's maturity in metrics 19 and 30.

TIC 3.0

Third, HUD did not transition from TIC 2.0 to TIC 3.0 as was reported in our FY 2023 FISMA evaluation. TIC 3.0 provides enhanced flexibility for agencies to route their network traffic through a trusted

¹¹ 2020-OE-0001, HUD FY 2020 FISMA Evaluation Report, Recommendations 15 and 16 (November 30, 2020). <https://www.hudoig.gov/reports-publications/report/hud-fiscal-year-2020-federal-information-security-modernization-act>.

¹² 2023-OE-0001-17, HUD FY 2023 FISMA Evaluation Report, Recommendation 17 (January 29, 2024). <https://www.hudoig.gov/reports-publications/report/hud-fy-2023-federal-information-security-modernization-act-fisma>.

connection. OMB M-19-26 required agencies to update their policies and procedures to address TIC 3.0 by September 2020. HUD did not achieve this deadline, but it reported that it implemented the Remote Access use case in quarter 2 of FY 2024. HUD also reported that it had completed engineering and transition activities in FY 2025 for the Branch Office use case, which was planned for a pilot in FY 2026. OIG did not evaluate the specifics of the implementation as provided in HUD's comments to our draft report, as the TIC 3.0 metric was not assessed this year. However, at the time of our evidence collection in April 2025, HUD did not provide this evidence or close the associated TIC 3.0 recommendation.

While this is primarily an issue of noncompliance with the OMB directive, it stands as an example of HUD not adapting to changing InfoSec requirements, which could have larger consequences in other areas. Although HUD has made good progress in addressing the new InfoSec requirements in FY 2025, as noted above, it has not resolved some of its older InfoSec improvement needs, including this one as an example. HUD has an open recommendation to define its TIC 3.0 strategy (2021-OE-0001-13).¹³ Implementing TIC 3.0 would improve HUD's maturity in metric 7.

Automated GRC Tool

Finally, HUD did not implement an automated GRC tool, which would remove manual processes in updating risk information. Manual processes are a risk to HUD's stakeholders in making effective decisions, because they could result in untimely or inaccurate information. An automated process, when configured correctly, reduces the risk of decision making based on untimely or inaccurate data, which can lead to better outcomes across HUD's InfoSec program. HUD's CDM tool, discussed earlier in the key initiatives section, is an example where automation drives updated information for decision making. HUD has an open recommendation to implement an automated GRC tool (2024-OE-0002-02).¹⁴ Implementing an automated GRC tool would improve HUD's maturity in metric 12.

Integration of HUD's Cybersecurity Assessment and Management (CSAM) Application and the System Security Dashboard

HUD continued to use its (b) (5) to track and report information on the security posture of its IT systems. However, the SSD relied in part on manual data entry from CSAM. Although HUD and the Department of Justice (DOJ) worked to integrate the information contained in CSAM with the SSD through an application programming interface (API) that would automate the data flow process, HUD and the DOJ did not complete this integration in FY 2025. Timely and accurate cybersecurity information is a key requirement for HUD stakeholders to make informed decisions in managing the InfoSec program. Data sharing via an API would ensure timely visibility into system vulnerabilities, patch management status, and other critical security indicators. Additionally, this automation would reduce the dependency on manual data handling, which would lower the risk of inaccurate data and make reporting processes more efficient and reliable. Continuing to implement this integration would enhance the effectiveness and reliability of data reporting, which HUD could then use to establish a data-driven approach to IT system management. Integrating the data from CSAM into the

¹³ 2021-OE-0001-17, FY 2021 FISMA Evaluation Report, Recommendation 17 (February 17, 2022).

<https://www.hudoig.gov/reports-publications/report/fiscal-year-2021-federal-information-security-modernization-act-fisma>.

¹⁴ 2024-OE-0002-02, HUD FY 2024 FISMA Evaluation Report, Recommendation 2 (October 29, 2024).

<https://www.hudoig.gov/reports-publications/report/hud-fy-2024-federal-information-security-modernization-act-fisma>.

SSD using an automated API would improve HUD's maturity in several metrics, including metrics 7-9, 12, 14-15, and 26-28.

Integration of HUD's Enterprise-Wide Business Impact Analysis (EWBIA) and Contingency Planning

HUD did not align the results of the EWBIA with its list of mission-essential functions (MEF) and high-value assets (HVA). Doing so would ensure that HUD has one consistent plan to recover systems in the event of a cybersecurity incident, instead of having two plans that weren't aligned with each other. If an incident were to occur, conflicting plans could lead to a delay in HUD's recovery due to the need to determine which plan to follow. Making those decisions ahead of time instead of during an incident would improve the effectiveness of the recovery process.

In FY 2025, HUD updated its EWBIA. The EWBIA served as a prioritized list of HUD systems to recover in the event of a cybersecurity incident. Individual system-level business impact analyses were consolidated into the EWBIA. As HUD modernizes, develops, and decommissions IT systems, the list and prioritization of systems in the EWBIA need reviewed. Updating the EWBIA was an important step for HUD to ensure the prioritization for system recovery represented current business requirements, as these priorities could change over time as new systems were developed and old ones were decommissioned.

HUD also needs to consider system dependencies in the EWBIA. If a system is dependent on another system to function, then the dependent system cannot be recovered until the system that it relies on has recovered first. A consideration of system dependencies would inform how HUD should focus its recovery efforts. And, as noted above, it would be better for HUD to make these determinations prior to the need to perform the actual recovery in a real cybersecurity incident. HUD has two open recommendations, 2022-OE-0001-04 and 2023-OE-0001-23, related to this topic.¹⁵ Resolving the issues noted above would improve HUD's maturity in metric 33.

Data Inventory

The FY 2025 IG FISMA metrics contained a new supplemental metric related to inventorying data. Like the discussion above about securing IT systems and assets, HUD must have awareness of the data it possesses to ensure that the data is properly secured. HUD determined its approach to build a catalog of data across the agency, including metadata attributes to collect. HUD had developed a roadmap for creating its data catalog and revised its data governance structure to move the Chief Data Officer into OCIO. However, this approach was not developed into formal policies and procedures that would help communicate to stakeholders what HUD required for collecting and tagging data resources across the agency.

HUD was implementing an initial capability to identify the data contained in systems listed in IAS. HUD reported that it obtained contractor support for this project in August 2025. After developing the initial data catalog that covered systems listed in IAS, HUD stated that future development of its data inventory

¹⁵ 2023-OE-0001-23, HUD FY 2023 FISMA Evaluation Report, Recommendation 23 (January 29, 2024).

<https://www.hudoig.gov/reports-publications/report/hud-fy-2023-federal-information-security-modernization-act-fisma>.

2022-OE-0001-04, HUD FY 2022 FISMA Evaluation Report, Recommendation 4 (September 30, 2022).

<https://www.hudoig.gov/reports-publications/report/hud-fy-2022-federal-information-security-modernization-act-fisma>.

would cover systems outside of IAS in the WASP¹⁶ and unstructured data, such as data that is not in a database. As HUD develops its data catalog, it will be in a better position to secure its data resources.

We issued a report on HUD's management of personally identifiable information (PII) in December 2024. The report contains useful information for HUD to consider in developing its data inventory. For example, we found that HUD had not determined the volume of PII that it managed. An effective data catalog would include this information. We made recommendations that cover areas that HUD should address to improve the effectiveness of its data inventory and its data protection and privacy program, including metrics 10, 21, and 22.¹⁷

HUD's Implementation of a File Integrity Monitoring Solution

HUD previously reported in our FY 2024 evaluation that it planned to implement a file integrity monitoring tool. This tool would allow HUD to know when changes were made to a file by comparing a file's hash signature to a known value that the file should have based on its contents. HUD planned to use the file integrity monitoring tool for several purposes across the agency. First, as an incident detection tool, it could identify when files were unexpectedly changed, which could be an indicator of an attack. Second, HUD intended to use the tool to ensure that custom-code applications maintained the correct configuration settings, since a change in the configuration settings would cause a change in the file data.

However, HUD personnel reported a challenge that the volume of files HUD needed to monitor exceeded their capability to use their intended tool effectively. HUD personnel were considering switching to another tool for this purpose. HUD was also coordinating with the DHS CDM team to consider other appropriate and cost-effective options. HUD's challenges in implementing a file integrity monitoring tool were like those it faced in implementing MFA as noted above. HUD selected a solution, began to implement the chosen solution, and then discovered issues that resulted in a new approach to addressing the problem. This resulted in a delay in addressing the underlying problem and wasted effort in implementing the solution that did not meet HUD's needs. Using a file integrity monitoring tool for its intended purposes would help improve HUD's maturity in metrics 14, 15, and 30.

¹⁶ As noted above, HUD does not include web applications in the IAS inventory, but instead web applications are inventoried in a separate SharePoint site, the WASP.

¹⁷ 2023-OE-0007, HUD PII Risk Management in a Zero Trust Environment, Recommendations 3 and 5 (December 12, 2024). <https://www.hudoig.gov/reports-publications/report/us-department-housing-and-urban-development-personally-identifiable>.

Conclusion and Recommendations

Based on our evaluation, HUD's InfoSec program was determined to be not effective, although HUD continued to improve overall. We assessed HUD at maturity level 3, consistently implemented, based on our evaluation of the 20 core metrics and the 5 new FY 2025 supplemental metrics within the 10 domains from the FY 2025 IG FISMA reporting guidance. 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 increased in maturity for 4 metrics and decreased in maturity for one metric, representing a net increase of 3 maturity levels. In addition, HUD was at maturity level 3, consistently implemented, for 4 of the 5 new supplemental metrics, and at maturity level 2, defined, for the remaining new supplemental metric. HUD maintained the same overall maturity rating at level 3, consistently implemented, but the incremental improvements that we observed in FY 2025 increased its score rating within that maturity level.

HUD improved maturity in one domain, reaching maturity level 3, consistently implemented, for the C-SCRM domain because it implemented its vendor assessment program. This allowed HUD to have awareness of the risks from its IT suppliers. HUD also achieved maturity level 3, consistently implemented, for the new Cybersecurity Governance domain and the associated Govern function. Achieving this maturity level in the new domain and function the first year represented how HUD had the ability to adapt to changing cybersecurity requirements.

However, HUD continued to show limitations in addressing longstanding cybersecurity weaknesses. HUD has made significant progress over the past several years in closing FISMA recommendations and should continue to prioritize recommendation closures to improve its cybersecurity posture.¹⁸

RECOMMENDATIONS

We provide 13 recommendations to improve the effectiveness of HUD's InfoSec program and assist HUD in increasing its maturity level within the IG FISMA metrics, domains, and NIST CSF 2.0 functions. We make recommendations in this report that guide HUD up to achieving maturity level 4, managed and measurable, because OMB defines this maturity level as an effective level of InfoSec maturity.

We recommend that HUD's Office of the Chief Information Officer:

- 1A. Coordinate with HUD Enterprise Risk Management to ensure alignment with HUD's overall risk strategy, formalize and implement its policies and procedures for maintaining current and target cybersecurity profile(s) with the NIST CSF 2.0 to include consideration of HUD's objectives, threat landscape, resources (including personnel), constraints, scope, changes to HUD's overall security posture, and the assessment of gaps between the current and target cybersecurity profile(s) (FY 2025 IG FISMA metric 1).
- 1B. Coordinate with other program offices as necessary to ensure that cybersecurity objectives are included in the performance assessment process of individuals with significant cybersecurity

¹⁸ For details on HUD's progress in closing recommendations from prior FISMA evaluations, see Appendix B.

responsibilities regardless of their position in HUD’s organizational structure (FY 2025 IG FISMA Metric 3).

- 1C. Monitor and analyze performance measures on the effectiveness of cybersecurity risk management roles based on established cybersecurity objectives to make updates as appropriate (FY 2025 IG FISMA metric 3).
- 1D. Coordinate with the Office of the Chief Procurement Officer to develop, collect, and communicate quantitative and qualitative performance measures to monitor the performance of cybersecurity supply chain risk management products, systems, and services (FY 2025 IG FISMA metric 5).

1E. [REDACTED]

1F. Use automation to make appropriate modifications in a timely manner to the security configurations of all IT systems and components connected to the HUD network (FY 2025 IG FISMA metric 14).

1G. [REDACTED]

1H. Develop, collect, and communicate quantitative and qualitative performance measures to monitor the performance of its flaw remediation processes (FY 2025 IG FISMA metric 15).

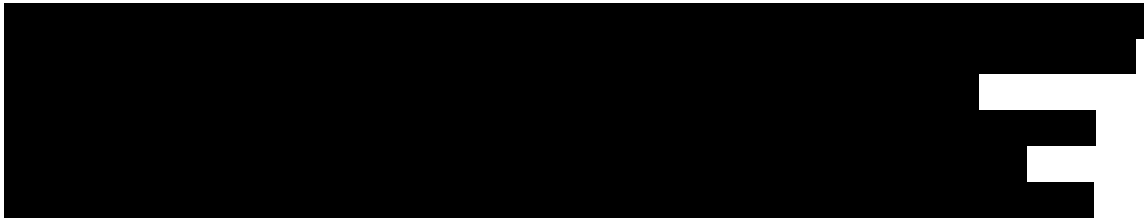
1I. [REDACTED]

¹⁹ [REDACTED]

2018-OE-0003-08, HUD FY 2018 FISMA Evaluation Report, Recommendation 8 (October 31, 2018). <https://www.hudoig.gov/reports-publications/report/hud-fiscal-year-2018-federal-information-security-modernization-act>.

1J. Ensure that the data collected for ISCM metrics are obtained accurately, consistently, and in a reproducible manner, such as by leveraging automation (FY 2025 IG FISMA metric 26).

1K.



1L. Implement sufficient automated monitoring for ISCM technologies that HUD leverages or conduct manual reviews for technologies that cannot be sufficiently monitored through automation and document the results of these reviews for future review (FY 2025 IG FISMA metric 27).

1M. Coordinate with HUD’s Enterprise Risk Management to ensure that the results of system-level BIAs and the EWBIA are integrated with ERM processes for evaluating, recording, and monitoring the sensitivity and criticality of IT assets (FY 2025 IG FISMA metric 33).

Management Response

OCIO provided eight comments to our report. Three of the OCIO’s comments asked us to reconsider recommendations that we planned to issue and the remaining five comments requested changes to the wording of the report. OCIO provided additional context on their progress in implementing MFA, TIC 3.0 use cases, and HUD’s Data Catalog. OCIO also provided additional information on the timeline of resuming its ISCM assessment program and the potential impacts of the temporary suspension of ISCM assessments.

OIG Evaluation of Management Response

Based on OCIO’s comments, we agreed to remove one recommendation that was targeted at maturity level 4, managed and measurable. Although we did not assess the associated metric at that maturity level in our FY 2025 evaluation, the intent of the recommendation was to guide HUD towards the requirements at maturity level 4. Based on OCIO’s response that they are currently using cyber threat intelligence and log analysis to support the metric requirements, we hope to see progress in the associated metric to maturity level 4 in FY 2026. If our future evaluations determine that there is a weakness in this area, we will issue appropriate recommendations at that time.

We did not remove the other two recommendations that OCIO requested. Both recommendations target weaknesses in written policies and procedures at maturity level 2, defined, in their respective metrics. OCIO provided evidence of implementation, which is important, but does not eliminate the need for effective policies and procedures. The first recommendation that OCIO requested to remove was related to its vulnerability scanning program for web applications. HUD’s IT Security Control Catalog, Vulnerability Management Procedures, and relevant stakeholders during our interview and data collection processes all referred to a requirement for web applications to be scanned “at least annually,” which was insufficient to meet the BOD timelines that the recommendation references. The evidence

that OCIO provided showed six scans that had not been performed in the last two weeks. Aligning HUD's policies and procedures with the BODs would create a HUD requirement for more frequent scanning that OIG could verify implementation of in future evaluations.

The second recommendation that OCIO requested to remove was related to defining specific roles and responsibilities for certain InfoSec tasks. OIG agrees that HUD personnel were performing the identified tasks, and the associated metric was assessed at maturity level 3, consistently implemented. The basis of the recommendation was to formally define the roles and responsibilities for performing these tasks, which would ensure that there was a basis to hold personnel accountable for those tasks.

We also made some changes to the wording of the report to include the additional information that OCIO provided to us on MFA, TIC 3.0 use cases, HUD's Data Catalog, and the ISCM assessment program. For MFA, we also added context that OCIO's information refers to planned actions in FY 2026-2027 that have not been completed yet. We disagree with OCIO's interpretation of OMB M-19-26; however, our findings were also justified from the IG FISMA metrics which required HUD to "[define] and [customize], as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies..."

We added information about HUD's Data Catalog based on the evidence that we received, and we also included the fact that HUD's Chief Data Officer is now in OCIO. Finally, for the ISCM program, we did not make any changes to our report based on the FY 2026 lapse in appropriations.

Scope, Methodology, and Limitations

We completed this evaluation under the authority of the Inspector General Act of 1978, as amended, and in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency (December 2020).²⁰ The Quality Standards require that we plan and perform evaluations in a manner that allows us to obtain sufficient and appropriate evidence that provides a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence that we have obtained from HUD provides such a reasonable basis for our findings and conclusions.

SCOPE

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, 2024, to September 30, 2025.²¹

METHODOLOGY

Fieldwork was based on the FY 2025 IG FISMA Reporting Metrics²² and associated CyberScope reporting questions. We assessed 20 core metrics and 5 supplemental metrics in FY 2025. We selected a sample of information systems from HUD's IAS 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.
- queries of HUD's CSAM system to obtain system artifacts.
- interviews and demonstrations to gain an understanding of information security, privacy, data protection programs and practices, and system operations.

²⁰ CIGIE Quality Standards for Inspection and Evaluation (December 2020).

<https://www.ignet.gov/sites/default/files/files/QualityStandardsforInspectionandEvaluation-2020.pdf>

²¹ This narrative report is based on our FY 2025 CyberScope report, which is provided below in Appendix D. The CyberScope report was issued to HUD on July 30, 2025. However, to the extent the Department provided additional information after the CyberScope report was submitted, we considered it and updated this narrative report accordingly.

²² 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.

- 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.
- 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 2025 supplemental metrics across six program office systems, which are listed in figure 6 below.

Figure 6 – List of FY 2025 FISMA sample systems²³

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

SAMPLE SYSTEM DESCRIPTIONS FROM SSPS AND HUD’S IAS

(b) (5)

²³ Abbreviations used in this summary table are defined in the following paragraphs or in the “system acronym” column of this table. Further, (b) (5)

(b) (5) [Redacted]

(b) (5) [Redacted]

(b) (5) [Redacted]

(b) (5) [Redacted]

(b) (5) [Redacted]

(b) (5)



REPORTING

We compiled the information necessary to address the specific reporting requirements outlined in OMB M-25-04, FY 2025 Guidance on Federal Information Security and Privacy Management Requirements.²⁴ Responses to specific FY 2025 IG FISMA reporting metrics were submitted through the DHS CyberScope application and are provided in appendix D of this report.

LIMITATIONS

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

²⁴ M-25-04, FY 2025 Guidance on Federal Information Security and Privacy Management Requirements (January 15, 2024). <https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf>.

Appendixes

APPENDIX A – MANAGEMENT RESPONSE

OCIO's Management Response



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, D.C. 20410-3000
OFFICE OF THE CHIEF INFORMATION OFFICER

December 11, 2025

MEMORANDUM FOR: Christeen Thomas, Director, Evaluation Division, Office of the Inspector General

FROM: Juan Sargeant, Deputy Chief Information Officer

SUBJECT: HUD comments on Draft FY 2025 FISMA Evaluation (2025-OE-0001)

This memorandum is in response to the Office of the Inspector General (OIG) draft report *Draft FY 2025 FISMA Evaluation (2025-OE-0001)*. The Office of the Chief Information Officer (OCIO) has carefully reviewed the Draft Report and provided comments.

If you have questions or require additional information, please contact William Trull, OCIO Audit Liaison Officer at william.n.trull@hud.gov or Erika McKinley, Supervisory IT Project Manager at erika.mckinley@hud.gov.

Enclosure:
HUD Comments for Draft Report FY 2025 FISMA Evaluation (2025-OE-0001)

**JUAN
SARGEANT**

Digitally signed by: JUAN SARGEANT
DN/CN = JUAN SARGEANT C = US O
= U.S. Government OU = Department
of Housing and Urban Development,
Office of the Chief Information Officer
Date: 2025.12.11 15:28:02 -05'00'

Juan Sargeant
Deputy Chief Information Officer
U.S. Department of Housing and Urban Development

Date

HUD Comments for Draft Report FY 2025 FISMA Evaluation (2025-OE-0001)

Security Operation Center Updates for the New Recommendations Issued

1. Page 16, Line #511, **Recommendation 1I**: “Update policies and procedures for scanning web applications in accordance with the requirements of DHS binding operational directives (BOD) 19-02, 22-01, and 23-01 to support the detection and remediation of vulnerabilities within required timelines and then implement its scanning program for web applications in accordance with the BOD requirements (FY 2025 IG FISMA metric 15).”

HUD Response: HUD runs web application scans every two weeks as a standard practice in accordance with the following Binding Operational Directives (BODs):

- a) BOD 1902: Vulnerability Remediation Requirements for Internet-Accessible Systems
- b) BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities
- c) BOD 2301: Improving Asset Visibility and Vulnerability Detection on Federal Networks

Because CISA BODs are mandatory for all government agencies, HUD does not need a departmental policy or procedure to require compliance with the directives. Due to the sensitive nature of the information, the evidence will be submitted separately to the OIG.

OIG Action: Please identify your concerns and/or evidence to support this new recommendation, and if this is a mistake, please remove the recommendation.

2. Page 17, Line #519, **Recommendation 1K**: “Define specific roles and responsibilities for monitoring the integrity and security posture of all IT assets, including (1) collecting and analyzing data on security incidents to understand associated risks and threat actor activity; (2) monitoring and enforcing the manual isolation or disconnection of non-compliant IT assets; (3) using network monitoring capabilities based on known indicators of compromise to maintain situational awareness; and (4) correlating information from multiple sources for analysis and monitoring (FY 2025 IG FISMA metric 27).”

HUD Response: HUD leverages threat intelligence from DOJ, CISA, and Mandiant to collect and analyze security incidents and threat actor activity. HUD isolates threats during incident response via CrowdStrike and maintains situational awareness through network monitoring based on known compromise indicators. Due to the sensitive nature of the information, the evidence will be submitted separately to the OIG.

OIG Action: Please identify your concerns and/or evidence to support this new recommendation, and if this is a mistake, please remove the recommendation.

3. Page 17, Line #526, **Recommendation 1L**: “Use timely cyber threat intelligence and log analysis tools to improve the accuracy of detecting cyber events, characterize threat actors, threat methods, and indicators of compromise (FY 2025 IG FISMA metric 27).”

HUD Response: HUD Cyber Threat Intelligence feeds the HUD CSOC Cyber Threat Hunt team to improve the accuracy of detecting cyber events, characterize threat actors, threat methods, and indicators of compromise. Due to the sensitive nature of the information, the evidence will be submitted separately to the OIG.

OIG Action: Please identify your concerns and/or evidence to support this new recommendation, and if this is a mistake, please remove the recommendation.

Spotlight on Key Initiatives

4. Page 5, Line #106: **Spotlight on Key Initiatives**

HUD Response: The *Program Improvement Needs* section on page 10, Line #317 details HUD’s MFA difficulties, but the *Spotlight on Key Initiatives* section on page 5, Line #106 omits HUD’s progress in this area. Due to the sensitive nature of the information, the evidence will be submitted separately to the OIG.

OIG Action: Add the following under *Spotlight on Key Initiatives* section.

HUD drives Zero Trust ICAM modernization under OMB, DHS, and NIST guidance. It delivers identity prerequisites, achieves Initial Operating Capabilities (IOC), and (b) (5). In 2025, HUD delivered critical ICAM prerequisites and Initial Operating Capabilities (IOC) required before enterprise-wide MFA enforcement, including deploying Phishing Resistant MFA for nine FHA Connection (FHAC) systems supporting lenders and business partners (~95,000 users).

TIC 3.0

5. Page 11, Line #343: “Third, HUD did not transition from TIC 2.0 to TIC 3.0 as M-19-26 required HUD to do by September 2020.”

HUD Response: The above finding is incorrect. The Office of Management and Budget (OMB) memo, M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*, September 12, 2019, requires agencies to “within one year of the release of this memorandum, agencies shall complete updates to their own network and system boundary policies to reflect this memorandum”. The memo does not direct agencies to transition to TIC 3.0 by September 2020. Due to the sensitive nature of the information, the evidence will be submitted separately to the OIG.

OIG Action: Change the wording to say the following:

HUD missed the September 2020 deadline to update policies for TIC 3.0 plans but fully implemented the TIC 3.0 Remote Access use case in FY 2024 Q2 2024. HUD also

completed major engineering and transition activities (b) (5)
(b) (5)

Cover Memo

6. Page ii, 2nd paragraph: *“However, until the transition is completed and ISCM assessments resume, this will be an area of concern due to OCIO not having timely cybersecurity information available to guide executives in their decision making and allocation of a limited pool of resources to the IT systems with the greatest needs for those resources.”*

HUD Response: We believe the sentence above is inaccurate as executives already have timely cybersecurity information available through CSAM to guide their decision making. Notifications are instantaneous to Deputy CIO/CIO after triage of incident validity is complete. Reporting to CISA is within one hour.

OIG Action: Please identify your timing concerns and/or evidence to support this finding, and if this is a mistake, please remove the finding.

7. Page ii, 2nd paragraph: *“The primary weakness that we identified in FY 2025 was the suspension of the InfoSec Continuous Monitoring (ISCM) program. OCIO reported that this suspension was temporary while systems completed the transition from NIST Special Publication (SP) 800-53, Rev. 4 controls to Rev. 5 controls.”*

HUD Response: HUD has begun ISCM planning and will launch initial assessments in January 2026, expanding them over time.

OIG Action: Replace every instance of ‘suspended/suspension’ with the phrase ‘pause/paused during furlough’, due to Program Office staff not being available.

Program Improvement Needs – Data Inventory

8. Page 21, Line #399 (Program Improvement Needs) Data Inventory: *“The FY 2025 IG FISMA metrics contained a new supplemental metric related to inventorying data. Like the discussion above about securing IT systems and assets, HUD must have awareness of the data it possesses to ensure that the data is properly secured. HUD determined its approach to build a catalog of data across the agency, including metadata attributes to collect. However, this approach was not developed into formal policies and procedures. Creating data inventory policies and procedures would help communicate to stakeholders what HUD required for collecting and tagging data resources across the agency.”*

HUD was implementing an initial capability to identify the data contained in systems listed in IAS. HUD expected to have contractor support for this project by the end of FY 2025. After developing the initial data catalog that covered systems listed in IAS, HUD stated that future development of its data inventory would cover systems outside of IAS in the

WASP and unstructured data, such as data that is not in a database. As HUD develops its data catalog, it will be in a better position to secure its data resources.”

We issued a report on HUD’s management of personally identifiable information (PII) in December 2024. The report contains useful information for HUD to consider in developing its data inventory. For example, we found that HUD had not determined the volume of PII that it managed. An effective data catalog would include this information. We made recommendations that cover areas that HUD should address to improve the effectiveness of its data inventory and its data protection and privacy program, including metrics 10, 21, and 22.”

HUD Response: HUD recently awarded the contract on August 12, 2025, and developed a roadmap for creating a data catalog baseline with initial schema, lineage, and controls. HUD also developed a revised data governance structure and approach to develop a unified sensitive taxonomy for the agency’s data assets. We will submit a closure package for priority recommendation 2023-OE-0007-03: “The CDO should coordinate with HUD’s Records Office, Privacy Office, and program offices to develop data policies and procedures for data inventory, categorization, and labeling in support of zero trust architecture,” later this month. It is also important to note that the CDO function has been recently transferred to the OCIO.

OIG Action: Please see the proposed edits to the Data Inventory section under Program Improvement Needs as follows:

“The FY 2025 IG FISMA metrics contained a new supplemental metric related to inventorying data. HUD awarded the contract on August 12, 2025, and developed a roadmap for creating a data catalog baseline with initial schema, lineage, and controls. HUD also developed a revised data governance structure and approach to develop a unified sensitive taxonomy for the agency’s data assets. HUD should also create data inventory policies and procedures that would help communicate to stakeholders what HUD requires for collecting and tagging data resources across the agency.

HUD was implementing an initial capability to identify the data contained in systems listed in IAS. After developing the initial data catalog that covered systems listed in IAS, HUD stated that future development of its data inventory would cover systems outside of IAS in the WASP and unstructured data, such as data that is not in a database. As HUD develops its data catalog, it is important to include the volume of PII it manages and fully implement data protection measures accordingly.

We issued a report on HUD’s management of personally identifiable information (PII) in December 2024. The report contains useful information for HUD to consider in developing its data inventory. HUD took a significant first step to address some of the concerns in the report. HUD should continue to improve the effectiveness of its data inventory and its data protection and privacy program, including metrics 10, 21, and 22.”

APPENDIX B – PRIOR FISMA RECOMMENDATIONS

Summary of Prior FISMA Recommendations

HUD OIG has issued 138 recommendations in prior FISMA evaluations since FY 2018.²⁵ Of the 138 FISMA recommendations, 42 recommendations were still open as of September 30, 2025. Figure 7 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.

Figure 7 – Summary of prior open FISMA recommendations by domain and FY

Domain ²⁶	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	FY 2023	FY 2024	Domain Total
Cybersecurity governance	(b) (5)	(b) (5)	(b) (5)	(b) (5)	(b) (5)	(b) (5)	(b) (5)	(b) (5)
Cybersecurity supply chain risk management								
Risk and asset management								
Configuration management								
Identity and access management								
Data protection and privacy								
Security training								
InfoSec continuous monitoring								
Incident response								
Contingency planning								
Fiscal year total	1	1	8	10	3	15	4	42

Details of each of the open recommendations from prior FISMA evaluations are provided at the end of this appendix.

We show HUD’s overall progress in closing recommendations by FY of the previous FISMA report in figure 8, below. In FY 2025, HUD closed 33 recommendations, including 19 FISMA recommendations. In

²⁵ All recommendations from older FISMA reports, including FY 2014 through FY 2017, have been closed. Therefore, we no longer report on those FISMA recommendations. We also note that there are recommendations from other evaluation reports that are not FISMA recommendations that HUD should also address.

²⁶ Cybersecurity governance was first created as a domain in the FY 2025 FISMA evaluation, so it has no recommendations shown in this table that were issued in prior FISMA evaluations. Cybersecurity supply chain risk management was first created as a domain in the FY 2021 FISMA evaluation, so it has no recommendations before that evaluation.

addition, HUD closed one priority recommendation²⁷ in FY 2025 and closed one priority recommendation in late FY 2024 that was not previously reported.²⁸ 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.

Figure 8 – FISMA evaluation recommendation closure status

FY of FISMA evaluation	Number of recommendations issued	Number of open recommendations, end of FY 2025	Number of closed recommendations, end of FY 2025	Number of recommendations closed in FY 2025
2018	30	1	29	2
2019	26	1	25	2
2020	26	8	18	1
2021	23	10	13	7
2022	5	3	2	1
2023	23	15	8	5
2024	5	4	1	1
Total	138	42	96	19

List of Open FISMA Recommendations from Prior Evaluations

We provide the following list of recommendations that remained open from prior FISMA evaluations as of September 30, 2025. Where possible, we have updated the reference to FISMA metric numbers to the most recent metric number available. Some recommendations may apply to multiple domains, but they will only be listed once under the primary domain that applies to the recommendation.

Cybersecurity Governance



²⁷ Priority recommendations are the recommendations that HUD OIG believes will have the greatest impact on helping HUD achieve its mission if they are implemented. Information on all priority recommendations can be found at <https://www.hudoig.gov/priority-open-recommendations>. For FISMA recommendations that are also priority recommendations, these are recommendations that we have identified as having a significant impact on the improvement of HUD’s InfoSec program.

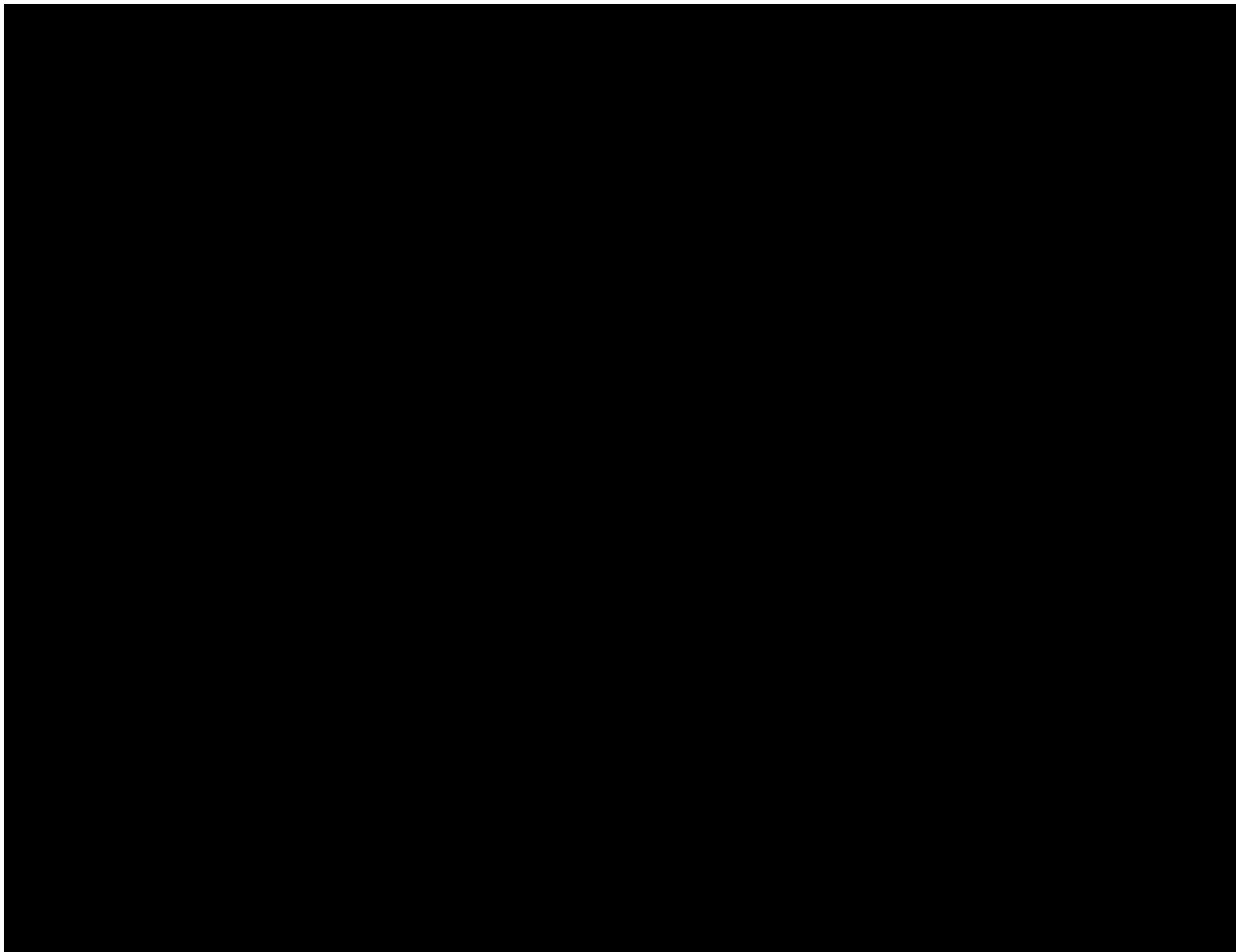
²⁸ Due to the timing of the cycle of the annual CyberScope report and this narrative report, recommendations that HUD closes in quarter 4 of each fiscal year may not be reflected until the following year’s report. For priority recommendations, however, we want to ensure that we also note HUD’s progress in closing the recommendation in the text as well as the tables.

Cybersecurity Supply Chain Risk Management



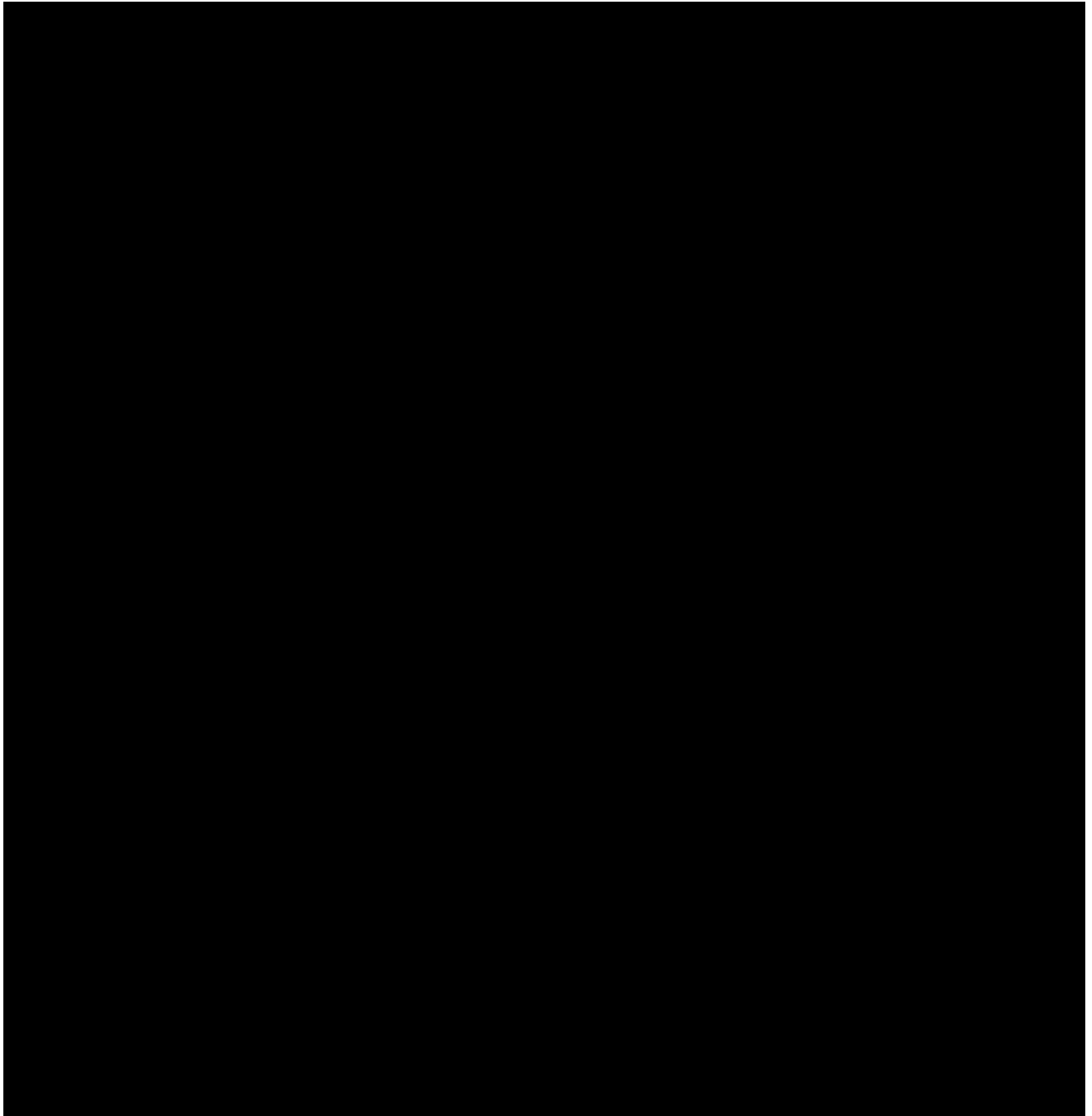
Risk and Asset Management

- **FY 2020 FISMA, Recommendation 1 (Priority Recommendation):** HUD OCIO should implement a software asset management capability for software and operating systems to ensure that software executes only from the authorized software inventory (whitelisting) and all unauthorized software is blocked from executing on HUD's network (FY 2025 IG FISMA metric 9).

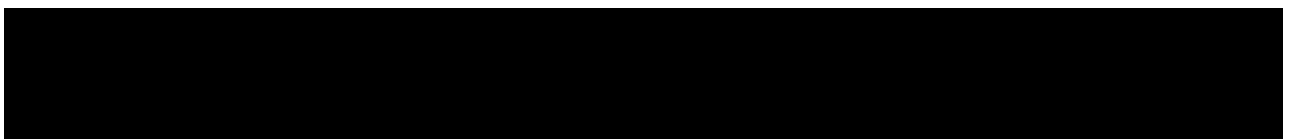


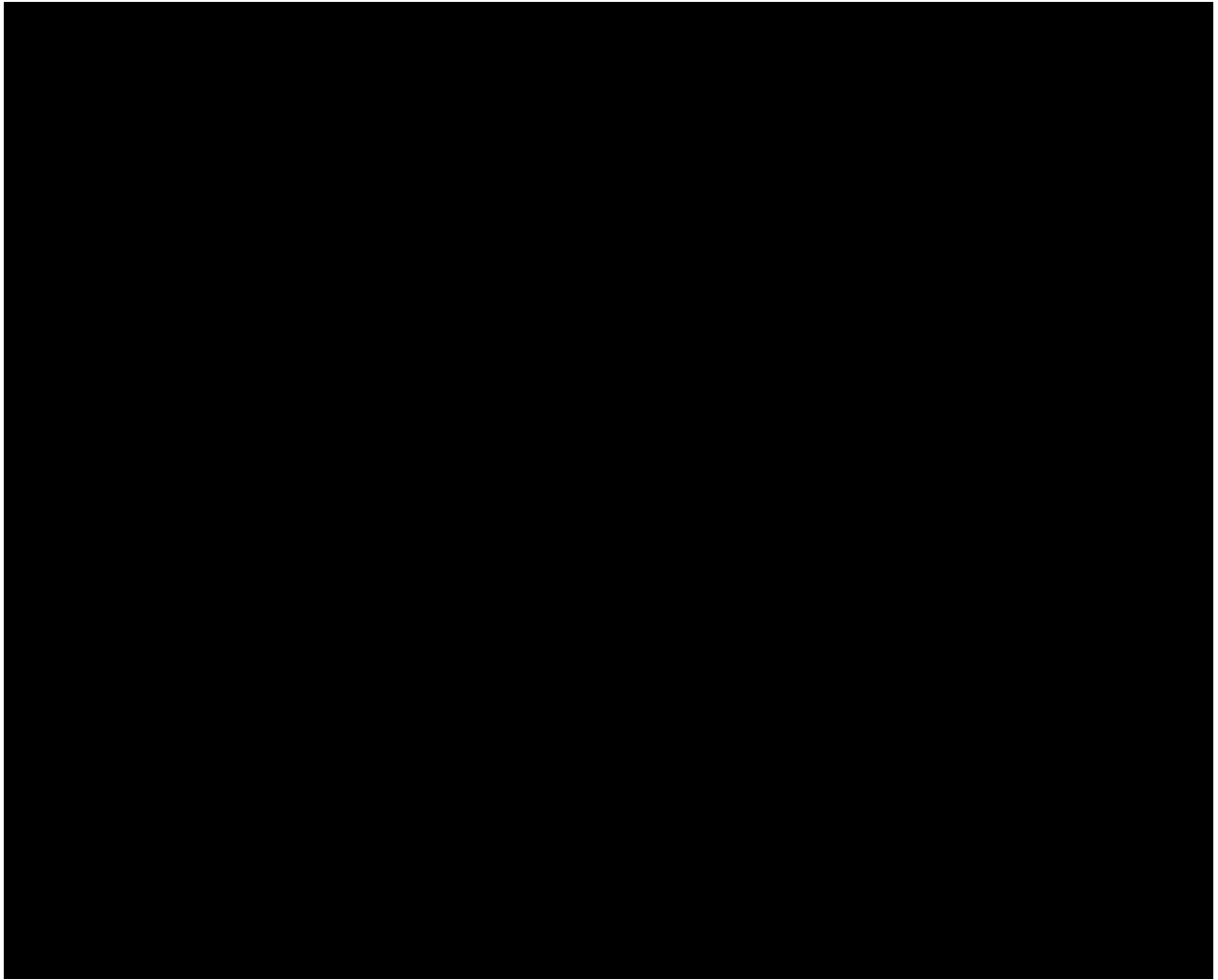
- **FY 2022 FISMA, Recommendation 2:** HUD OCIO and the HUD Chief Risk Officer should coordinate to implement procedures to monitor the effectiveness of cybersecurity risk

responses to ensure that risk tolerances are maintained at an appropriate level (FY 2025 IG FISMA metric 11).

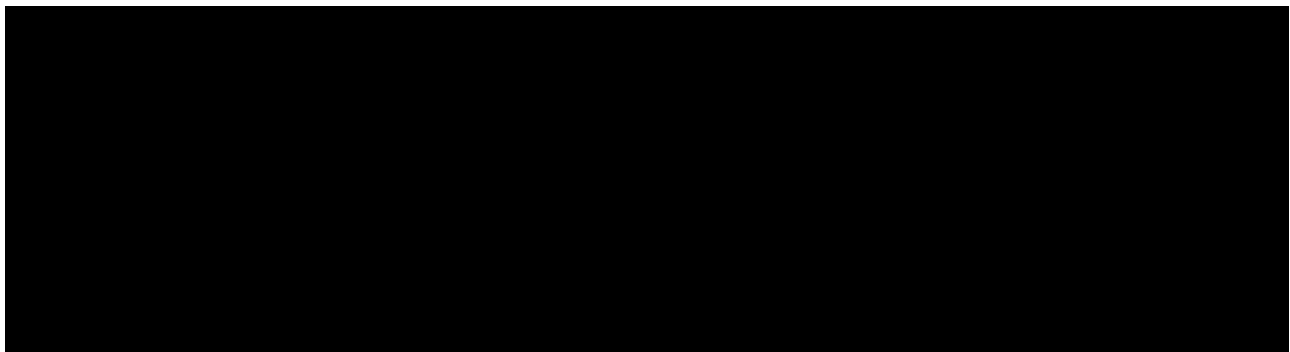


Configuration Management



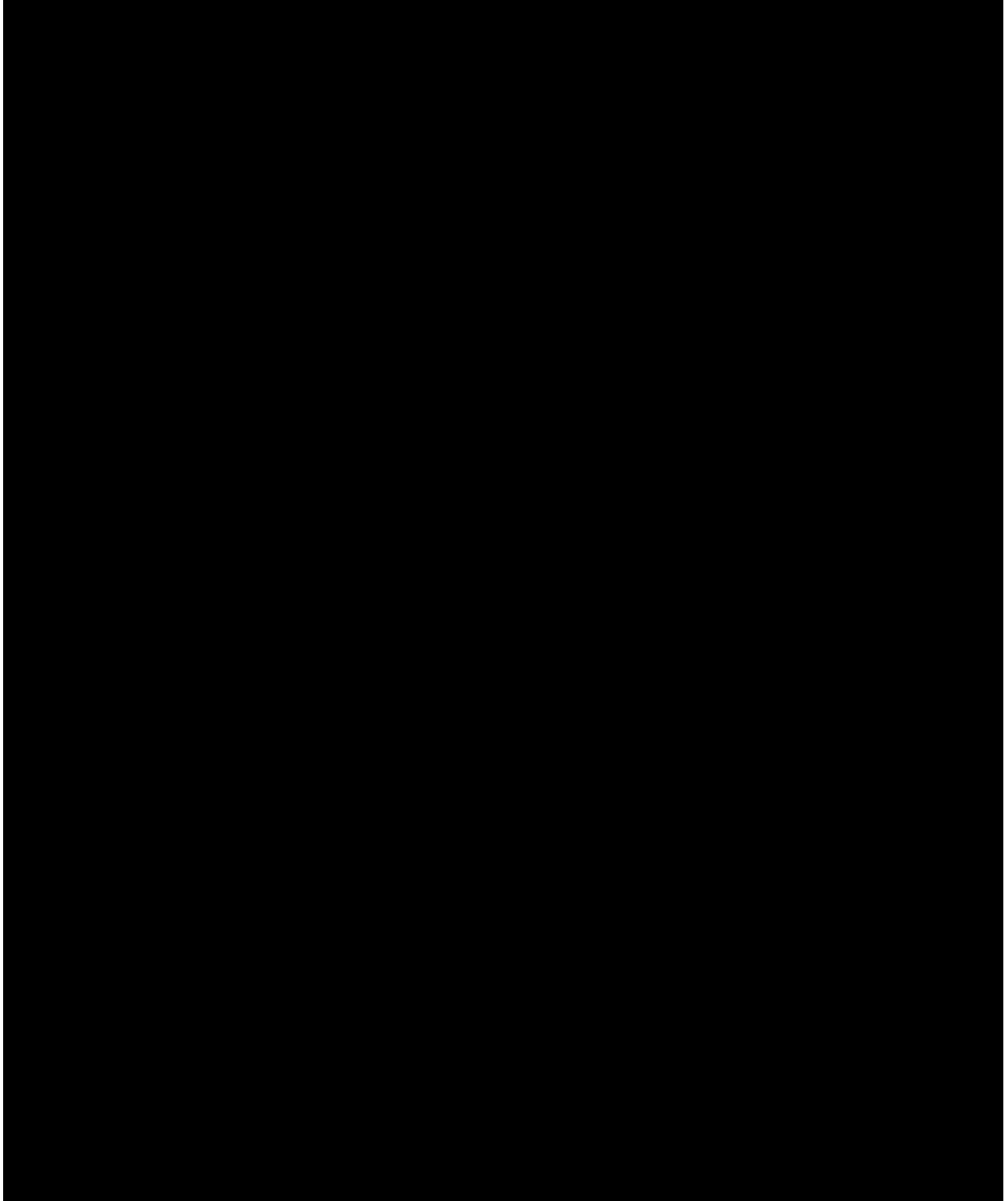


Identity and Access Management



- **FY 2020 FISMA, Recommendation 15 (Priority Recommendation):** HUD OCIO should implement multifactor authentication mechanisms for all nonprivileged users who access information systems that process, store, or transmit PII (FY 2025 IG FISMA metric 17).

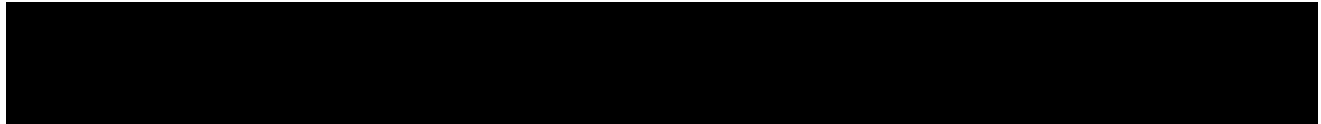
- **FY 2020 FISMA, Recommendation 16 (Priority Recommendation):** HUD OCIO should implement multifactor authentication mechanisms for all privileged users who access information systems that process, store, or transmit PII (FY 2025 IG FISMA metric 18).



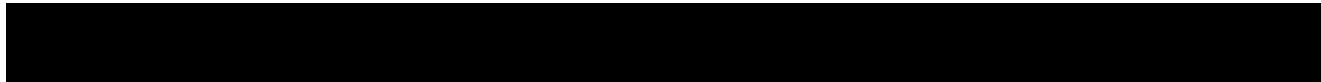
Data Protection and Privacy



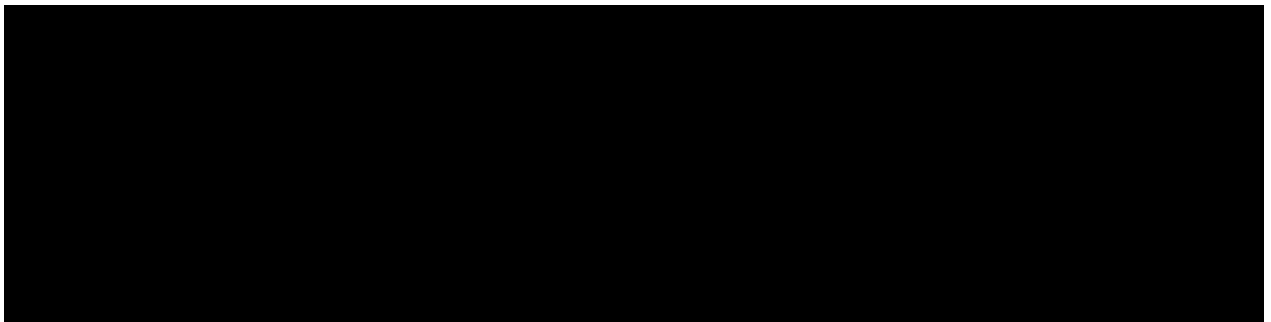
Security Training



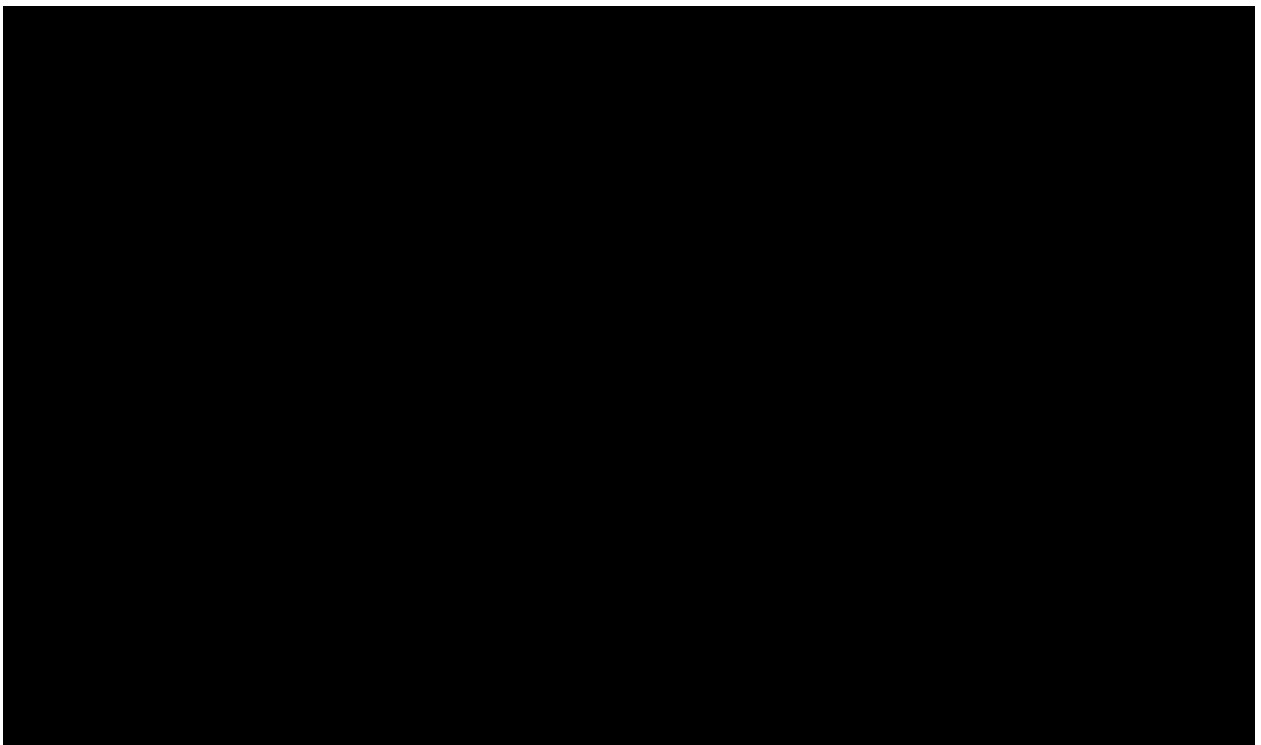
Information Security Continuous Monitoring



Incident Response



Contingency Planning



APPENDIX C – ABBREVIATIONS

Abbreviations	Definition
API	application programming interface
AUS	automated underwriting system
BOD	binding operational directives
BYOD	bring-your-own-device
CDM	continuous diagnostics and mitigation
(b) (5)	
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	configuration management
CSAM	cybersecurity assessment and management
CRO	Chief Risk Officer
CSF	cybersecurity framework
C-SCRM	cybersecurity supply chain risk management
EIDAM	enterprise identity and access management
EL	event logging
EO	executive order
EWBIA	enterprise-wide business impact analysis
DHS	Department of Homeland Security
DOJ	Department of Justice
(b) (5)	
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GFE	government-furnished equipment
(b) (5)	
GRC	governance risk and compliance
(b) (5)	

Abbreviations	Definition
HUD	U.S. Department of Housing and Urban Development
(b) (5)	
HVA	high-value asset
IAS	inventory of automated systems
IG	Inspector General
InfoSec	information security
ISCM	InfoSec continuous monitoring
IT	information technology
MEF	mission-essential function
MFA	multi-factor authentication
NIST	National Institute of Standards and Technology
OCFO	Office of Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OCPO	Office of the Chief Procurement Officer
(b) (5)	
PII	personally identifiable information
PMO	project management office
ROB	rules of behavior
SCRM	supply chain risk management
SOC	security operations center
SP	special publication
(b) (5)	
SSP	system security plan
TIC	trusted internet connection
TMF	Technology Modernization Fund

APPENDIX D – FY 2025 HUD OIG CYBERSCOPE SUBMISSION

Appendix D contains HUD OIG’s responses to the FY 2025 IG FISMA metrics that were established by OMB. OMB issued M-25-04, FY 2025 Guidance on Federal Information Security and Privacy Management Requirements, on January 15, 2025. M-25-04 contains details on required FISMA reporting instructions. HUD OIG submitted the FY 2025 CyberScope submission to the DHS CyberScope application on July 29, 2025.

The subsequent section of the report is not being publicly released due to concerns about the risk of circumvention of the law: Appendix D, FY 2025 HUD OIG Cyberscope Submission.

APPENDIX E – HUD FISMA METRIC TRENDS

The 20 core metrics have been assessed each year since FY 2022, so they can be used to measure HUD’s progress in improving its InfoSec maturity over time, unlike the supplemental metrics which have each been assessed once. In the core metrics, HUD had a net increase of 3 maturity levels this year and a net increase of 15 maturity levels since FY 2022. Figure 9 shows the core metric maturity trends since FY 2022 with green up arrows indicating an increase in maturity from FY 2022 and yellow horizontal arrows indicate no change since FY 2022.

Figure 9 – Core metric maturity trends since FY 2022

FY 2025 Metric #	Previous Metric # ²⁹	FY 2022 Rating	FY 2023 Rating	FY 2024 Rating	FY 2025 Rating	Net Change from FY 2022
5	14	Ad hoc	Ad hoc	Defined	Consistently implemented	↑↑
7	1	Defined	Defined	Defined	Consistently implemented	↑
8	2	Consistently implemented	Defined	Managed and measurable	Consistently implemented	↔
9	3	Consistently implemented	Defined	Consistently implemented	Consistently implemented	↔
11	5	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented	↔
12	10	Defined	Defined	Defined	Defined	↔
14	20	Defined	Defined	Consistently implemented	Consistently implemented	↑
15	21	Defined	Defined	Defined	Consistently implemented	↑
17	30	Defined	Ad hoc	Defined	Defined	↔
18	31	Defined	Ad hoc	Defined	Defined	↔
19	32	Defined	Defined	Defined	Consistently implemented	↑
21	36	Defined	Defined	Consistently implemented	Consistently implemented	↑

²⁹ Although the core metrics have not changed, they were renumbered in FY 2025.

FY 2025 Metric #	Previous Metric # ²⁹	FY 2022 Rating	FY 2023 Rating	FY 2024 Rating	FY 2025 Rating	Net Change from FY 2022
22	37	Defined	Consistently implemented	Managed and measurable	Managed and measurable	
24	42	Consistently implemented	Consistently implemented	Managed and measurable	Managed and measurable	
26	47	Defined	Consistently implemented	Consistently implemented	Consistently implemented	
28	49	Defined	Consistently implemented	Consistently implemented	Consistently implemented	
30	54	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented	
31	55	Consistently implemented	Consistently implemented	Managed and measurable	Managed and measurable	
33	61	Consistently implemented	Consistently implemented	Consistently implemented	Consistently implemented	
34	63	Defined	Consistently implemented	Managed and measurable	Managed and measurable	