

A photograph of classical stone columns and arches of a building, likely a government or institutional structure, in the background. A thick yellow curved line separates the image from the white background below.

CFPB: 2026 Information Security Program Audit



Report Highlights

CFPB: 2026 Information Security Program Audit



Why This Matters

The Consumer Financial Protection Bureau maintains databases containing millions of consumer complaints, sensitive financial information, and confidential supervisory records on financial institutions. The CFPB must protect this information from increasingly sophisticated cyber threats that could jeopardize the confidentiality and integrity of data crucial to the agency's mission.

Key Results

According to federal metrics for evaluating agencies' information security programs, the CFPB's information security program is not effective. It has a maturity level of 2 out of a possible 5, meaning its program is defined but not consistently implemented. We found weaknesses in several areas:

- Asset inventories have gaps, multiple actively used datasets are not recorded in the data inventory, and hardware at vacated regional offices is not properly inventoried and potentially not secure. These issues could limit the CFPB's ability to protect resources and share information with other federal agencies.
- Risk management framework processes with outdated baseline controls and reactive vulnerability management hinder the effectiveness of the CFPB's information security program—for example, the CFPB failed to remediate critical and high-severity vulnerabilities within required 30-day time frames but later made plans to address these vulnerabilities.
- Policies and guidance have gaps or are outdated in multiple areas, including the agency's cybersecurity risk strategy, security policies, and business impact analyses for nine newly authorized systems.

Further, 10 of 14 unresolved recommendations from our prior annual information security audits remain open. We are currently reviewing evidence the CFPB submitted after the conclusion of our fieldwork to determine whether to close 9 of the 10 open recommendations.

Action Needed

We have 8 new recommendations to strengthen asset management, risk framework implementation, and policy governance. The CFPB agreed with our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Contents

Introduction.....	5
Objective	5
Background	5
FISMA Maturity Model.....	7
Summary of the CFPB’s 2026 FISMA Maturity Rating.....	9
Finding 1: Deficiencies in Asset Inventories Limit Information Security and Resource Protection.....	10
Inconsistent Tracking of Data Assets Reduces Visibility into Security and Use of Information.....	10
Unvalidated Regional Hardware Assets Leave Property and Data Potentially Unsecured.....	11
Unconfirmed Interconnection Inventory Presents Risks to Information Systems	11
Finding 2: Inconsistencies in Risk Management Framework Processes Hinder Information Security Program Effectiveness.....	13
Inaccurately Documented NIST Baseline Controls May Leave Systems Vulnerable to Cyber Threats.....	13
Inconsistent Change Management Documentation May Reduce Awareness of Security and Privacy Impacts	14
Vulnerabilities Are Not Consistently Tracked and Timely Remediated, Increasing Exposure to Cyber Threats.....	14
Finding 3: Policy Gaps and Outdated Guidance Inhibit Efforts to Enhance FISMA Maturity and Security Posture	16
Missing Elements of an Organizational Cybersecurity Strategy Impede Enterprisewide Risk Management Activities.....	16
Outdated Policies Prevent Higher FISMA Maturity.....	17
Conclusion and Recommendations	18
Agency Response and Our Evaluation	20
Appendix A: Scope and Methodology.....	21
Appendix B: Status of Prior Recommendations.....	24

Appendix C: Agency Response	28
Abbreviations.....	32

Introduction

The Consumer Financial Protection Bureau is responsible for regulating the offering and provision of consumer financial products and services under relevant laws. To conduct its work, the CFPB maintains databases containing millions of consumer complaints, sensitive financial information, and confidential supervisory records on financial institutions. Under the Federal Information Security Modernization Act of 2014 (FISMA), the CFPB is required to implement cybersecurity controls to protect these critical systems and data from increasingly sophisticated cyber threats.

Objective

In accordance with FISMA requirements, our audit objectives were to evaluate the effectiveness of the CFPB's (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines. Our scope and methodology are detailed in appendix A.

Background

FISMA requires agencies to develop, document, and implement an agencywide security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or another source.¹ FISMA also requires that each inspector general (IG) perform an annual independent evaluation to determine the effectiveness of the information security program and practices of their respective agency, including testing the effectiveness of information security policies, procedures, and practices for selected systems.

To support independent evaluation requirements, the Office of Management and Budget (OMB), the Council of the Inspectors General on Integrity and Efficiency, and other stakeholders collaborated to develop the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.² In March 2026, OMB and the Council of the Inspectors General on Integrity and Efficiency directed IGs to use the *FY 2025 IG FISMA Reporting Metrics* for fiscal year (FY) 2026 evaluations. Previously, reporting metrics were generally updated each year.

¹ Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–3558).

² Office of Management and Budget, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, April 3, 2025.

The IG FISMA reporting metrics are grouped into 10 security domains, which align with the 6 function areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework.³ The 6 function areas are *govern, identify, protect, detect, respond, and recover*. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks. Each of these function areas and domains include a number of metrics that IGs are required to assess using a maturity model (table 1).⁴

Table 1. NIST Cybersecurity Framework Functions, Outcomes, and Associated Reporting Domains

Function	Cybersecurity outcomes	Associated IG FISMA reporting domain
<i>Govern</i>	Provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five functions in the context of its mission and stakeholder expectations.	Cybersecurity governance and cybersecurity supply chain risk management
<i>Identify</i>	Understands the organization’s assets, suppliers, and related cybersecurity risks to enable an organization to prioritize its efforts consistent with its risk management strategy.	Risk and asset management
<i>Protect</i>	Supports the ability to secure assets to prevent or lower the likelihood and impact of adverse cybersecurity events.	Configuration management, identity and access management, data protection and privacy, security training
<i>Detect</i>	Enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring.	Information security continuous monitoring
<i>Respond</i>	Supports the ability to contain the effects of cybersecurity incidents.	Incident response

³ National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, February 26, 2024.

⁴ As noted in the *FY 2025 IG FISMA Reporting Metrics*, IGs use the CyberScope application to submit the results of their metrics evaluation, including maturity level ratings. As such, we reported our detailed responses and assessment of the CFPB’s progress in implementing these metrics in CyberScope. Because of the sensitive nature of our responses, they are restricted and not included in this report.

Function	Cybersecurity outcomes	Associated IG FISMA reporting domain
<i>Recover</i>	Supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.	Contingency planning

Source: Office of Management and Budget, *FY 2025 IG FISMA Reporting Metrics*.

FISMA Maturity Model

Each function area, domain, and metric area is assessed using a five-level maturity model:

1. *ad hoc*
2. *defined*
3. *consistently implemented*
4. *managed and measurable*
5. *optimized*

The foundational levels (1–3) of the model are geared toward the development and implementation of policies and procedures, and the advanced levels (4–5) capture the extent to which agencies institutionalize those policies and procedures. As noted in the *FY 2025 IG FISMA Reporting Metrics*, in the context of the maturity model, OMB believes that achieving a level 4 (*managed and measurable*) or above represents an effective level of security.⁵ Metric, domain, and function level maturity ratings factor into the overall determination of whether an agency's information security program is effective (figure 1). Further details on the scoring methodology for the maturity model are included in appendix A.

⁵ NIST defines security and privacy control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the designated security and privacy requirements. National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Revision 5, December 10, 2020.

Figure 1. IG FISMA Maturity Model



Source: Office of Management and Budget, *FY 2025 IG FISMA Reporting Metrics*.

Summary of the CFPB's 2026 FISMA Maturity Rating

For FY 2026, the CFPB's information security program operates at a level-2 (*defined*) maturity, which does not meet the level-4 (*managed and measurable*) effectiveness standard established by OMB. This assessment reflects persistent challenges facing the CFPB: incomplete asset inventories that limit visibility into resources requiring protection, inconsistent risk management framework processes evidenced by inaccurately documented NIST baseline controls and reactive vulnerability management, and policy gaps and outdated guidance. Combined with a significant backlog of unresolved recommendations from our prior audits, these issues prevent the CFPB from improving the maturity level of its information security program.

We note that the CFPB has experienced decreased staffing levels since 2024, which has hindered the agency's ability to perform key activities.⁶ Specifically, enterprisewide risk management activities were suspended in March 2025, but responsibilities were reassigned as of June 2026. In the information standards team, departures have required remaining members to absorb additional responsibilities, resulting in delayed vulnerability plan of action and milestones (POA&M) reviews and a reactive rather than proactive approach to tracking security weaknesses. Data inventory management is now conducted by one person, limiting the agency's ability to maintain comprehensive visibility into the data assets it is responsible for protecting.

Further, 10 of the 14 unresolved recommendations made in prior years' FISMA audit reports remain open; however, we are reviewing closure packages for each of these open recommendations that the CFPB provided after the conclusion of our fieldwork. Many of these recommendations address foundational control weaknesses. Persistent unresolved recommendations in areas like cybersecurity risk registers, data classification and loss prevention, vulnerability remediation tracking, and contingency planning prevent the CFPB from demonstrating the consistent implementation and effectiveness required to achieve higher maturity levels. Until these recommendations are fully implemented, the CFPB will continue to face challenges in establishing the managed and measurable security posture necessary for an effective information security program (appendix B).

⁶ According to the CFPB's semiannual report to Congress, 524 of 1,758 employees departed the agency from September 30, 2024, to December 31, 2025.

Finding 1: Deficiencies in Asset Inventories Limit Information Security and Resource Protection

The CFPB has gaps in its asset inventory management processes that reduce visibility into the agency's information technology (IT) resources. The agency does not consistently track data assets, cannot validate the security of hardware located in former regional offices, and lacks processes to ensure its system interconnections inventory is complete and accurate.⁷ These deficiencies limit the CFPB's ability to have a comprehensive view of its data and metadata, protect hardware and data from unauthorized access, and manage security risks associated with information sharing between systems and external federal agencies.

Inconsistent Tracking of Data Assets Reduces Visibility into Security and Use of Information

We found gaps in the CFPB's data inventory management. A *data inventory* is a comprehensive catalog of all datasets collected, stored, and used to track critical information like data owners, sensitivity levels, personally identifiable information (PII), and use. However, the CFPB's data inventory tool contains gaps, with multiple actively used datasets not recorded in the data inventory. In addition, during our audit period, we found that over 50 additional datasets were awaiting CFPB staff verification that those datasets are being used by the agency. As a result, neither we nor the CFPB could verify whether these assets are in use.⁸

FISMA and NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, require agencies to maintain inventories of organizational systems and data assets to ensure adequate visibility and management of the IT environment. The *FY 2025 IG FISMA Reporting Metrics* further requires that agencies maintain complete and accurate inventories of data and corresponding metadata for designated data types.

According to CFPB personnel, the team responsible for reviewing and updating the CFPB's data inventory has been reduced to one person, and the CFPB has not documented policies or procedures for how often the data inventory should be reviewed and updated. Without a comprehensive data inventory and proper identification and classification of PII within datasets,

⁷ A *system interconnection* is a direct connection between two or more systems in different authorization boundaries for the purpose of exchanging information or allowing access to information, information services, and resources.

⁸ We are reviewing supporting evidence provided by the CFPB to close this finding.

the CFPB does not have full visibility into the data and metadata it is responsible for, where they are being stored, or what is being done with them.

Unvalidated Regional Hardware Assets Leave Property and Data Potentially Unsecured

CFPB officials informed us that the agency left hardware assets at its former regional offices, which were vacated in 2025, and that occupancy and lease administration responsibilities for those former offices are managed by the U.S. General Services Administration. CFPB officials informed us that they retained ownership and responsibility for the IT assets that remained at these locations. They also informed us in June 2026, and reconfirmed in early September 2026, that the agency has not verified whether those hardware assets, which the CFPB remains accountable for, are appropriately secured.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, requires organizations to enforce physical access authorizations at entry and exit points to the facility where hardware assets are located and to verify individual access authorizations before granting access. It also requires organizations to use asset-location technologies to track and monitor the location and movement of system components in controlled areas and to detect unauthorized movement or removal of organizational assets.

On September 30, 2026, we issued a management alert recommending that the CFPB's chief information officer (CIO) ensure that the hardware assets located at the former regional office spaces are appropriately accounted for and secured.⁹ The CIO, in the agency's official response to the management alert, stated that the CFPB had already begun a full, site-by-site IT decommissioning at the former regional offices. The CIO stated that all decommissioning activities were expected to be completed by September 30, 2026. We are reviewing additional documentation the CFPB provided in October 2026 about its hardware assets located at the former regional offices.

Unconfirmed Interconnection Inventory Presents Risks to Information Systems

The CFPB lacks processes to ensure its system interconnections inventory is comprehensive. The agency uses a SharePoint authorization library as a repository for systems' interconnection security agreements. An *interconnection security agreement* is a document that specifies the technical and security requirements for establishing, operating, and maintaining an interconnection between two or more systems. While this approach provides a centralized storage location, and the agreements themselves contain required information, the CFPB does

⁹ Office of Inspector General, *CFPB: Hardware Assets at Former Regional Offices May Not Be Appropriately Secured*, [OIG Report 2026-IT-C-015](#), September 30, 2026.

not have a process to ensure the repository contains all required interconnection agreements. Further, the repository does not detail what systems require agreements, whether the agreements contain all required information, or the status of the review and update cycles for existing agreements.

OMB Circular A-130 and NIST SP 800-47, Revision 1, *Security Guide for Interconnecting Information Technology Systems*, require agencies to document and maintain interconnections between systems. NIST SP 800-53 Revision 5 requires organizations to authorize connections between information systems and to document each interconnection. The *FY 2025 IG FISMA Reporting Metrics* requires agencies to maintain complete inventories that include all systems and interconnections supporting organizational operations.

The CFPB does not have any documented policies or procedures related to maintaining an inventory of system interconnections. While the CFPB's system inventory tool includes dedicated fields for tracking whether systems require an interconnection security agreement, our review found these fields were marked "to be determined." Without a comprehensive inventory of system interconnections, the CFPB cannot effectively oversee and manage information sharing between its systems and external entities, which can result in unmanaged security risks.

Finding 2: Inconsistencies in Risk Management Framework Processes Hinder Information Security Program Effectiveness

The CFPB has inconsistently implemented the NIST risk management framework process, which FISMA requires agencies to follow to manage security and privacy risks.¹⁰ Several CFPB systems have inaccurately documented NIST baseline controls in the agency's governance, risk, and compliance (GRC) tool,¹¹ resulting in security plans being based on outdated criteria. The CFPB has also approved and implemented change requests without appropriately documenting the completed security risk and privacy impact assessments, increasing the risk that the agency's change control board would lack historical context on the impact to security or privacy controls. Finally, the CFPB has not consistently tracked and remediated vulnerabilities within required time frames, creating POA&Ms only after our inquiries rather than when the vulnerabilities became overdue. Without effective risk management framework implementation, the CFPB faces increased exposure to unauthorized access, undetected vulnerabilities, and security incidents.

Inaccurately Documented NIST Baseline Controls May Leave Systems Vulnerable to Cyber Threats

The CFPB's system documentation in its GRC tool has not been updated to reflect the use of newer NIST baseline controls. Of the four systems we sampled, three showed the use of the retired NIST 800-53, Revision 4, in the GRC tool. However, the CFPB was able to confirm that these systems had controls assessed under the current NIST 800-53, Revision 5, baseline in another security control assessment system.

NIST SP 800-53 provides a catalog of security and privacy controls for information systems and organizations. Agencies were required to use Revision 5 security control baselines starting in September 2020. Revision 5 changed a number of controls and introduced dedicated control families for PII and supply chain risk management. NIST SP 800-37, Revision 2, requires organizations to select security controls from the current version of NIST SP 800-53 when developing system security plans and conducting authorization activities.

¹⁰ The risk management framework process is established by NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*. It provides a flexible, holistic, and repeatable seven-step process to manage security and privacy risk and links to a suite of NIST standards and guidelines to support implementation of risk management programs for agencies to meet FISMA requirements.

¹¹ The CFPB uses GRC tools for documenting, managing, and status reporting of IT security risk assessments as well as the implementation of federal and NIST-developed IT security control standards and policies.

CFPB officials stated they had been focused on assessing the controls in their other assessment tool under NIST 800-53, Revision 5, and not consistently updating its GRC tool, which includes their older system security plans. System security plans based on outdated criteria may not adequately address current cybersecurity threats and vulnerabilities. The authorizing official may grant system authorization based on outdated security control baseline documentation, including for supply chain risk management and privacy controls.

Inconsistent Change Management Documentation May Reduce Awareness of Security and Privacy Impacts

We found inconsistencies in our review of change records for three sampled CFPB systems. For two of the six change records, the CFPB did not adequately document risk assessments or privacy impact analyses before implementing system changes. One of these change records clearly documented that an assessor did not assess potential privacy impacts, and the other change record had no information about the security and privacy impact analysis. The CFPB was able to provide evidence that the security and privacy impact analysis occurred for these two change records.

NIST SP 800-53, Revision 5, requires organizations to analyze changes for potential security and privacy impacts before implementation.

However, the CFPB had approved and implemented change requests without appropriately documenting the completed security and privacy impact assessments before change implementation. Without appropriately documenting security risk and privacy impact analyses before change implementation, the CFPB's change control board would lack historical context on the impact to security or privacy controls.

Vulnerabilities Are Not Consistently Tracked and Timely Remediated, Increasing Exposure to Cyber Threats

We continue to identify deficiencies in the CFPB's vulnerability management and remediation processes. An open recommendation from our 2024 FISMA audit report involves strengthening flaw remediation processes by developing and implementing a process to clearly map identified vulnerabilities to system internet protocol addresses, host names, and remediation owners in the CFPB's configuration management database.¹² In 2024, we found numerous critical and high-risk

¹² Office of Inspector General, *2024 Audit of the CFPB's Information Security Program*, [OIG Report 2024-IT-C-019](#), October 31, 2024.

operating systems and application vulnerabilities. The CFPB's internal vulnerability scans identified these issues, but the agency did not timely remediate them. In our 2025 FISMA report, we found instances of critical software platforms, along with software deployed to those platforms, that had reached their end of life and were no longer supported by vendors.¹³ This year, we found deficiencies in the CFPB's POA&M process. The CFPB's internal vulnerability scans identified overdue vulnerabilities and end-of-life software in June 2026, but the agency failed to create corresponding POA&Ms until we requested documentation. We further found that the CFPB did not remediate a significant number of critical and high-severity vulnerabilities within the required 30-day time frame.

NIST SP 800-53, Revision 5, requires organizations to remediate vulnerabilities within time periods defined by organizational policy. The CFPB's *Vulnerability Management Process—Standard Operating Procedure* establishes requirements for the timely remediation of critical and high-risk vulnerabilities. In addition, NIST SP 800-53, Revision 5, requires organizations to implement a POA&M process to document planned remediation actions to correct weaknesses identified during security control assessments.

CFPB officials informed us that, since March 2025, staff reductions in the information security standards team have required remaining members to absorb more responsibilities, delaying routine vulnerability POA&M creation and review. The CFPB's resulting reactive POA&M process caused overdue vulnerabilities without formal tracking or accountability for remediation. Critical and high-severity vulnerabilities that remain unpatched beyond required time frames create immediate risk to the agency's mission systems and increase the agency's vulnerability to cyber threats.

Because our 2024 FISMA recommendation remains open, we do not have a new recommendation for this issue.¹⁴

¹³ Office of Inspector General, *2025 Audit of the CFPB's Information Security Program*, [OIG Report 2025-IT-C-012](#), October 31, 2025.

¹⁴ We are reviewing supporting evidence provided by the CFPB to close this finding.

Finding 3: Policy Gaps and Outdated Guidance Inhibit Efforts to Enhance FISMA Maturity and Security Posture

The CFPB's information security policies and procedures do not reflect current federal requirements or operational practices, creating gaps that limit the agency's ability to effectively manage cybersecurity risk. The agency lacks required elements of an organizational cybersecurity risk strategy and has not developed, maintained, or updated select information security policies within required time frames. These policy deficiencies have contributed to inconsistent risk management practices across the organization, unclear accountability for risk management activities following organizational changes, and the absence of foundational guidance necessary for personnel to implement controls uniformly across systems. Because information security policies serve as the foundation for FISMA maturity levels, policy gaps and outdated guidance prevent the agency from achieving an effective information security program. Without current policies aligned with federal standards, the CFPB cannot ensure consistent security practices or make informed risk-based decisions.

Missing Elements of an Organizational Cybersecurity Strategy Impede Enterprisewide Risk Management Activities

We found that the CFPB's cybersecurity risk strategy lacks required elements and that enterprisewide risk management activities have been suspended because of departures of key personnel. An official stated that the CFPB was using several policies that together make up the agency's cybersecurity risk strategy, but the policies lack required elements like organizational risk tolerance, priorities, constraints, and assumptions. Further, CFPB staff stated that the agency was not aggregating and prioritizing risks across the organization appropriately, given that enterprise risk management (ERM) program activities have been suspended since March 2025. The CFPB assigned the chief risk officer role in June 2026. The agency also has open recommendations to address the absence of maintained cybersecurity risk registers to aggregate and prioritize risks across the organization as well as the lack of defined ERM roles, responsibilities, and strategy for cybersecurity profile development.

NIST SP 800-37 states that the risk management strategy guides and informs risk-based decisions, including how security and privacy risk is framed, assessed, responded to, and monitored. The risk management strategy may be composed of a single document or of separate security and privacy risk management documents. The risk management strategy

makes explicit the threats, assumptions, constraints, priorities, tradeoffs, and risk tolerance used for making investment and operational decisions. This strategy includes strategic decisions and considerations for how senior leaders are to manage security and privacy risks, including supply chain risks, to operations, assets, and personnel. NIST identifies that the risk management strategy should include organizational risk tolerance, acceptable risk assessment methodologies and risk response strategies, a process for consistently evaluating security and privacy risks organizationwide, and approaches for monitoring risk over time.

Agency risk policy calls for a standalone cybersecurity risk strategy that includes elements like organizational risk tolerance, priorities, constraints, and assumptions. However, the CFPB has not completed a comprehensive cybersecurity risk management strategy. Without a comprehensive strategy, the agency cannot make consistent, risk-informed decisions across the enterprise.

Outdated Policies Prevent Higher FISMA Maturity

We found gaps in the CFPB's policy maintenance, as two security policies in FISMA metric domains have not been reviewed or updated within required time frames. The asset management policy was updated in 2021, and the data access policy was updated in 2019, both of which exceed the required 2-year review cycle. The *Information Resource Resiliency* policy controlling the creation and management of system-level business impact analysis (SLBIA) lacks explicit requirements for SLBIA completion before granting authorization to operate (ATO). During our audit period, nine new systems were granted ATOs and onboarded without SLBIAs.

FISMA requires agencies to develop, document, and implement agencywide information security policies and procedures. The CFPB's *Information Security Standards* policy requires CFPB policies to be reviewed and updated at least every 2 years or following a significant organizational change or event. In addition, FISMA requires agency heads to implement risk-based policies and procedures and to cost-effectively reduce information security risks to an acceptable level.

Policy review and update processes have not been consistently executed. Further, the absence of formal policy documentation has led the CFPB to operate using an informal, undocumented process to conduct SLBIAs within a year of ATO. The CFPB risks operating on outdated guidance that does not reflect current technologies, threats, or operational requirements. Further, agency personnel lack the foundational guidance necessary to understand updated security requirements, make consistent decisions, or implement controls uniformly across systems, resulting in ad hoc approaches, inconsistent security postures, and gaps in protection. Because information security policies serve as the foundation for FISMA maturity levels, policy gaps and outdated guidance prevent the agency from progressing beyond a level-2 (*defined*) maturity rating to the level-4 (*managed and measurable*) or level-5 (*optimized*) maturity rating needed to demonstrate an effective information security program.

Conclusion and Recommendations

The CFPB's information security program operates at a level-2 (*defined*) maturity, falling short of the level-4 (*managed and measurable*) effectiveness standard set by federal guidance. Our assessment stems from three root causes: incomplete asset inventories that limit the CFPB's visibility into resources requiring protection; inconsistencies in risk management framework processes, evidenced by outdated NIST baseline controls and a reactive approach to vulnerability remediation; and security policies that have not kept pace with current standards and operational requirements. These weaknesses are further compounded by staff departures in key functions, including data inventory management and the information standards team, which have constrained CFPB's capacity to sustain core security processes. In addition, 10 of the 14 unresolved recommendations we made in prior years remain open.¹⁵ Many of these recommendations address foundational control weaknesses. To strengthen the CFPB's information security program, we have 8 new recommendations focused on three areas: (1) strengthening asset inventory management, (2) implementing effective risk management framework, and (3) aligning policies and guidance with current federal standards and operational practices. Implementing these recommendations will enable the CFPB to achieve comprehensive visibility into its security posture, consistently implement security controls across the enterprise, and effectively manage cybersecurity risks to agency information and information systems. After the conclusion of fieldwork, CFPB officials provided additional information related to proposed recommendations 1, 2, and 3. This information is currently under evaluation.

We recommend that the CIO

1. Update data inventory management policies and procedures to establish roles and responsibilities and frequency for review and update.
2. Assess data inventory management resources to ensure the CFPB's data inventory is comprehensive and up to date.
3. Develop and maintain policies and procedures for establishing and maintaining a comprehensive inventory of system interconnections, including frequency for review and update to interconnection security agreements.
4. Ensure that system security plans in the CFPB's GRC tool are updated with current NIST control baseline standards.
5. Strengthen change management process to ensure security and privacy impact analyses are appropriately documented before approving and implementing system changes.

¹⁵ We are reviewing the CFPB's corrective action plans for all open recommendations.

6. Enforce the review and updating of all security policies in alignment with CFPB policy.
7. Update the *Information Resource Resiliency* policy to require an SLBIA before granting an ATO and ensure that existing production systems without a SLBIA obtain one, as applicable.

We recommend that the chief risk officer, in conjunction with the CIO,

8. Ensure risk management strategy documents include enterprisewide risk tolerance, priorities, constraints, and assumptions.

Agency Response and Our Evaluation

In response to our official draft report, the CIO concurred with our findings and recommendations and conveyed the CFPB's commitment to addressing the items outlined in our recommendations. The agency's formal response to the report, included in full in appendix C, noted steps it had taken to enhance its cybersecurity posture after our audit fieldwork had ended, including submitting evidence to close 9 of the 10 open recommendations. As reflected in table B-1, we are currently reviewing the corrective action plans provided by the agency after the conclusion of our fieldwork.

The actions described by the CIO appear to be responsive to our recommendations. We will follow up with the CFPB quarterly to ensure that the recommendations are fully addressed.

Appendix A: Scope and Methodology

Our audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the CFPB's information security program and practices for FY 2026, as required by FISMA and OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*.

To conduct our work, we use the *FY 2025 IG FISMA Reporting Metrics* (Version 2.0, dated April 3, 2025), which aligns with the Cybersecurity Framework. The assessment uses a maturity model spectrum with five levels: *ad hoc* (level 1), *defined* (level 2), *consistently implemented* (level 3), *managed and measurable* (level 4), and *optimized* (level 5). In this context, achieving level 4 or above represents an effective level of security.

Our scope encompasses six Cybersecurity Framework function areas:

1. *Govern*: cybersecurity governance and cybersecurity supply chain risk management
2. *Identify*: risk and asset management
3. *Protect*: configuration management, identity and access management, data protection and privacy, and security training
4. *Detect*: information security continuous monitoring (ISCM)
5. *Respond*: incident response
6. *Recover*: contingency planning

The assessment period covers FY 2026, with our responses required for submission to the CyberScope reporting tool no later than July 30, 2026.

We used a calculated average approach wherein the average of metrics in a particular domain determines the effectiveness of individual function areas and the overall program. Calculated averages are not automatically rounded to a particular maturity level. We retain discretion to determine overall effectiveness based on core metric results; supplemental metric results as supporting data points; as well as other factors, such as results of other cybersecurity audits and evaluations conducted during the review period, progress in addressing outstanding recommendations, and security incidents reported during the review period.

To assess the effectiveness of the CFPB's information security program across all FISMA function areas, we

- conducted structured interviews with the chief information security officer, CIO, and senior IT leadership across all FISMA function areas. Interviews addressed policies, processes, implementation status, challenges, and progress on prior recommendations.
- reviewed policies, procedures, system security documentation, authorization packages, incident response plans, supplier risk assessment reports, and IT contracts.
- assessed documentation for formal approval, currency, distribution, required security and privacy clauses, and alignment with federal requirements.
- performed technical assessments across identity and access management (personal identity verification credentials, privileged access); asset inventories (systems, hardware, software, data); vulnerability management; network and endpoint monitoring; data protection controls; and ISCM program capabilities.
- evaluated incident response plans, contingency plans, and business impact analyses.

In addition, we selected nonstatistical, judgmental samples in select areas, described below. We selected each sample based primarily on specific risk factors unique to each population. The results cannot be projected to the full population. However, these samples informed our testing in the following security functions and were used in conjunction with additional testing to support our conclusions.

- **IT contract oversight:** We employed nonstatistical, judgmental sampling using risk-based criteria to select IT contracts for testing. From a population of 230 contract records totaling about \$273 million, we excluded zero-dollar obligations, non-IT contracts, and IT contracts below \$50,000. We selected four contracts valued at about \$106 million; those contracts represented 59.24 percent of eligible IT contract spend.
- **Risk management:** We used a census approach for reviewing all 20 risk acceptance system memorandums tested, representing 100 percent of the population.
- **Configuration management:** We applied nonstatistical, judgmental sampling using risk-based criteria to select systems for testing. We excluded non-PII systems, supporting services, low-impact systems, retired systems, expired or pending ATOs, and non-FISMA reportable systems. From an overall population of 48 systems, we identified 16 qualifying high-risk systems, 2 of which we selected for testing. We added 2 more systems based on our prior audit findings, yielding a total sample of 4 systems.
- **Authorization and continuous monitoring:** We applied nonstatistical, judgmental sampling using risk-based criteria to select systems for testing. We excluded non-PII systems, supporting services, low-impact systems, retired systems, expired or pending ATOs, non-FISMA reportable systems, and mission-essential function systems. From an

overall population of 48 systems, we identified 16 qualifying systems, 2 of which we selected for testing based on ATO process characteristics. We added 2 more systems based on our prior audit findings, yielding a total sample of 4 systems.

- **Change request review:** We applied nonstatistical, judgmental sampling to select change request records. From a population of 44 change request records, we selected 6 change request records associated with 3 sampled systems from a population of 48 systems for testing configuration management and security impact analysis controls.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted this work from May 2026 to October 2026.

Appendix B: Status of Prior Recommendations

Table B-1. Status of FISMA Recommendations That Were Open as of the Start of Our FY 2026 FISMA Audit, by Security Function

Year	Recommendation	Status	Explanation
Govern			
2025	1 We recommend that the acting CFPB director determine what ERM roles, responsibilities, and strategy components should be defined and leveraged for the development and maintenance of cybersecurity profiles.	Open	The CFPB has not determined what ERM roles, responsibilities, and strategy components should be defined and leveraged for the development and maintenance of cybersecurity profiles. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.
2025	3 We recommend that the chief operating officer, in conjunction with the CIO, develop policies and procedures to create and maintain cybersecurity profiles.	Open	The CFPB has drafted, but not finalized, a policy to create and maintain cybersecurity profiles. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.
Identify			
2022	4 We recommend that the CIO ensure that an enterprisewide software inventory is conducted and maintained.	Closed	The CFPB has implemented an enterprisewide software inventory process and provided documentation of its 2024 and 2025 annual software inventory and updated software listing. The CFPB maintains a centralized inventory integrated with other discovery systems.

Year		Recommendation	Status	Explanation
2024	8	We recommend that the CIO implement a process that ensures the cyber risk information in the CFPB's governance, risk, and compliance tool is accurate and maintained.	Open	The CFPB is not ensuring that its system inventory is capturing up-to-date system and risk information. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.
2025	2	We recommend that the chief operating officer, in conjunction with the CIO, develop and maintain cybersecurity risk registers to aggregate, normalize, and prioritize cybersecurity risks.	Open	The CFPB's cybersecurity risk registers are incomplete and are missing key elements. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.
2025	4	We recommend that the CIO perform a review of previously granted risk acceptance memorandums to determine whether they were based on a complete review of the system or common controls (as required by NIST Special Publication 800-37, Revision 2) and perform additional risk analysis and/or compensating controls as needed for affected systems.	Open	While the CFPB has made progress by significantly reducing systems operating under risk acceptance memorandums, it has yet to ensure that all previously issued systems with a risk acceptance memorandum receive either an ATO or an authorization to use or are decommissioned. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.
2025	5	We recommend that the CIO ensure that risk acceptance memorandums reflect an assessment of qualitative and quantitative cybersecurity risks, as applicable.	Closed	The CFPB has discontinued its risk acceptance memorandum process and has not issued any new risk acceptance memorandums since we made this recommendation.

Year		Recommendation	Status	Explanation
Detect				
2025	6	We recommend that the CIO evaluate options to perform ongoing information continuous monitoring activities commensurate with the current threat environment.	Open	The CFPB has not made sufficient progress toward implementing continuous monitoring commensurate with the current threat environment and has only evaluated options to perform ISCM activities for a limited number of systems. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.
Protect				
2018	3	We recommend that the CIO determine whether established processes and procedures for management of user-access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.	Closed	The CFPB has established a process for managing user-access agreements and rules-of-behavior forms for privileged users through the implementation of a new system that can manage these more effectively. This process is intended to be used for all FISMA-reportable systems and to assist in managing and tracking user-access agreements and rules-of-behavior forms, which were deemed sufficient to manage the control requirements.
2024	1	We recommend that the chief data officer complete finalization of an agencywide data classification policy that accounts for the sensitivity of the data maintained by the CFPB.	Open	The CFPB has drafted, but not finalized, an agencywide data classification policy that accounts for the sensitivity of the data maintained by the CFPB. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.
2024	2	We recommend that the CIO ensure that data classification and sensitivity labels are incorporated into the CFPB's data loss prevention program.	Open	The CFPB is in the process of finalizing its data classification policy. Based on this policy, the CFPB plans to fully incorporate data classification and sensitivity labels into its data loss prevention program. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.

Year		Recommendation	Status	Explanation
2024	3	We recommend that the CIO strengthen flaw remediation processes by developing and implementing a process to clearly map identified vulnerabilities to system IP addresses, host names, and remediation owners within the CFPB's configuration management database.	Open	We continue to identify that the CFPB did not remediate a significant number of critical and high-severity vulnerabilities within the required time frame established in the CFPB's vulnerability management process. Further, we found that the POA&M process did not adequately track and manage remediation timelines for identified vulnerabilities. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.
Recover				
2023	1	We recommend that the CIO, in coordination with business and mission stakeholders, maintain a comprehensive schedule for testing current contingency plans, documenting test procedures, and maintaining relevant updates to the contingency plan.	Closed	The CFPB has created a comprehensive schedule for testing contingency plans and established test procedures for its FISMA-reportable systems.
2024	6	We recommend that the chief administrative officer ensure that testing of mission-essential functions identified in the CFPB's continuity of operations plan is periodically performed.	Open	The CFPB is in the process of conducting contingency plan testing for its FISMA-reportable systems and related mission-essential functions. We are reviewing a corrective action plan provided by the CFPB to close this recommendation.

Appendix C: Agency Response



445 12th St SW, Washington, DC 20554

October 21, 2026

Mr. Andrew Gibson
Acting Assistant Inspector General for Information Technology
Board of Governors of the Federal Reserve System &
Consumer Financial Protection Bureau
20th and Constitution Avenue NW
Washington, DC 20551

Dear Mr. Gibson,

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the 2026 Audit of the CFPB's Information Security Program. We acknowledge that you found the Consumer Financial Protection Bureau's (CFPB) Information Security Program is at a level 2 (defined) maturity based on the Federal Information Security Modernization Act of 2014 (FISMA) maturity model. However, the report lacks important context as it does not fully recognize the security of the Bureau's systems and the significant improvements that the Bureau has made and continues to make in its cybersecurity posture. The audit process fails to account for enhancements completed after the audit field work ended nor does it provide credit for actions that the Bureau management took to improve information security that the review chose not to focus on.

Notably and most importantly, the Bureau did not have any major security incidents or breaches of personally identifiable information in FY 2026 despite facing increasingly sophisticated threats. Further, CFPB made substantial progress in closing out open recommendations. Of the 14 recommendations that were open when the audit field work commenced, four have been closed and the Bureau has submitted evidence to close nine of the remaining 10. That means that out of 14, only one remains. The two recommendations from OIG Report 2025-FMIC-C-013 on CFPB's asset management processes were also closed. The Bureau has made significant progress concerning issues raised by the OIG during this year's audit. In fact, of the eight recommendations in this year's report, CFPB has already submitted evidence documenting

consumerfinance.gov

implementation of three of them and anticipates closing all open findings by December 31, 2026. CFPB also resolved seven additional findings that OIG brought to its attention prior to the completion of field work and were therefore not addressed in this year's report.

Additionally, the Bureau made many improvements to its information security program that were not reflected in FISMA audit testing but meaningfully strengthened our cybersecurity posture. The Bureau tightened our technical controls, reduced the Bureau's attack surface, and deployed new technologies that better safeguard Bureau systems and data. Specific enhancements include a 55% reduction in vulnerabilities, decommissioning of 46 systems, implementation of multiple new web defense capabilities such as a super intelligence impersonator bot detection tool, deployment of improved solutions for asset monitoring and cloud security, and elimination 96% of servers with operating systems that were beyond end-of-life. These improvements were made systematically, following engineering best practices to ensure continuity of operations and data integrity. Although these actions do not affect the Bureau's FISMA score, they have materially hardened CFPB's infrastructure and demonstrate the Bureau's efforts to continuously improve the security and privacy of CFPB systems and data.

Moreover, the Bureau improved or created seven policies covering areas ranging from supply chain risk management to acceptable use of super intelligence, updated eight standard operating procedures including topics such as vulnerability management, contingency planning, and continuous monitoring, and implemented refreshed cybersecurity and privacy awareness training for all employees and contractors as well as specialized training for personnel with significant security responsibilities. Also, the CIO and CISO held meetings with system owners for all critical systems to ensure contingency planning and plan of action and milestones were being addressed in a timely manner. Collectively, the improved policies, procedures, training, and senior management attention reinforced the Bureau's commitment to a security aware culture and overall management of cybersecurity and privacy risks.

In summary, as our responses show, the Bureau has already done the work of addressing most of the OIG's recommendations and the Bureau will continue to focus its efforts on actions that impact on the security of its systems and data.

Sincerely,

**CHRISTOPHE
R CHILBERT**

Digitally signed by
CHRISTOPHER CHILBERT
Date: 2026.10.21 13:06:57
-04'00'

Christopher Chilbert
Chief Information Officer

Response to recommendations presented in the OIG Draft Report: 2026 Audit of the CFPB's Information Security Program

Recommendation 1: We recommend that CFPB update data inventory management policies and procedures to establish roles and responsibilities and frequency for review and update.

Management Response:

The CFPB concurs with this recommendation. CFPB has already implemented this recommendation and submitted supporting documentation to the OIG on September 22, 2026.

Recommendation 2: We recommend that the Chief Information Officer assess data inventory management resources to ensure the CFPB's data inventory is comprehensive and up to date.

Management Response:

The CFPB concurs with this recommendation. CFPB has already implemented this recommendation and submitted supporting documentation to the OIG on October 1st, 2026.

Recommendation 3: We recommend that the Chief Information Officer develop and maintain policies and procedures for establishing and maintaining a comprehensive inventory of system interconnections, including frequency for review and update to interconnection security agreements.

Management Response:

The CFPB concurs with this recommendation. CFPB has already implemented this recommendation and submitted supporting documentation to the OIG on September 29, 2026.

Recommendation 4: We recommend that the Chief Information Officer ensure that system security plans in the CFPB's governance, risk, and compliance tool are updated with current NIST control baseline standards.

Management Response:

The CFPB concurs with this recommendation. We expect to complete this by 12/31/2026.

Recommendation 5: We recommend that the Chief Information Officer strengthen change management processes to ensure security and privacy impact analyses are appropriately documented before approving and implementing system changes.

Management Response:

The CFPB concurs with this recommendation. We expect to complete this transition and make the applicable updates by 12/31/2026.

Recommendation 6: We recommend that the Chief Information Officer enforce the review and updating of all security policies in alignment with CFPB policy.

Management Response:

The CFPB concurs with this recommendation. We expect to complete this transition and make the applicable updates by 12/31/2026.

Recommendation 7: We recommend that the Chief Information Officer update the Information Resource Resiliency policy to require an SLBIA before granting an ATO and ensure that existing production systems without a SLBIA obtain one, as applicable.

Management Response:

The CFPB concurs with this recommendation. Evidence will be submitted for closure by 12/31/2026.

Recommendation 8: We recommend that the Chief Operating Officer, in conjunction with the Chief Information Officer, ensure risk management strategy documents include enterprise wide risk tolerance, priorities, constraints, and assumptions.

Management Response:

The CFPB concurs with this recommendation. We expect to complete this transition and make the applicable updates by 12/31/2026.

Abbreviations

ATO	authorization to operate
CIO	chief information officer
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GRC	governance, risk, and compliance
IG	inspector general
ISCM	information security continuous monitoring
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	personally identifiable information
POA&M	plan of action and milestones
SLBIA	system-level business impact analysis
SP	Special Publication



Hotline

Report fraud, waste, abuse, and mismanagement involving the programs and operations of the Board or the CFPB.

oig.federalreserve.gov/hotline

OIG Hotline

Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

1-800-827-3340

General Contact

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

202-973-5000

Media and Congressional Inquiries

oig.media@frb.gov