Audit Report
2025-IT-C-012
October 31, 2025

Consumer Financial Protection Bureau

2025 Audit of the CFPB's Information Security Program

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2025-IT-C-012, October 31, 2025

2025 Audit of the CFPB's Information Security Program

Findings

The Consumer Financial Protection Bureau's overall information security program has decreased from a level-4 maturity (*managed and measurable*) to a level-2 maturity (*defined*) in fiscal year 2025. We further concluded, based on the results of our determinations of effectiveness in each domain and function, that the CFPB's overall information security program is not effective. We found that the CFPB is not maintaining its authorizations to operate for many systems and is using risk acceptance memorandums without a documented analysis of cybersecurity risks. This issue has been compounded by the loss of contractor resources supporting information security continuous monitoring and testing activities and the departure of agency personnel. As such, the CFPB is unable to maintain an effective level of awareness of security vulnerabilities in its environment. We also found that the CFPB can strengthen its information security program by using cybersecurity profiles to assess, tailor, and prioritize its cybersecurity approach. Specifically, we believe that the use of profiles can help the agency align its cybersecurity program and control structure with the future state of the agency and the sensitive data it maintains.

We further found that, despite these resource and operating constraints, the CFPB was able to take some steps to maintain and strengthen its information security program. For example, the agency updated and formalized processes for responding to potential ransomware incidents and transitioned toward a continuous vetting model for employee background reinvestigations. Additionally, the senior agency information security officer continues to meet with system owners on a weekly basis to manage cybersecurity risks, and the agency is in the process of decommissioning and modernizing legacy technology systems.

Lastly, we continue to identify the use of outdated software on the CFPB's network for which vendors are no longer providing security updates and patches. A key reason for this issue is delays in modernizing, rearchitecting, and retiring legacy applications. We have previously raised this issue and have an open recommendation related to it. As such, we are not including a new recommendation and suggest that management prioritize efforts to reduce the risks resulting from the use of outdated software.

Recommendations

This report includes six new recommendations designed to strengthen the CFPB's information security program in the areas of cybersecurity profiles, security authorizations, and information security continuous monitoring. In response to a draft of our report, the CFPB concurs with our recommendations and notes that the recommendations will

Purpose

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the CFPB. Our specific audit objectives, based on legislative requirements, 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.

Background

FISMA requires each inspector general to conduct an annual independent evaluation of their agency's information security program, practices, and controls for selected systems. The Office of Management and Budget's (OMB) *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* directs inspectors general to evaluate the maturity level (from a low of 1 to a high of 5) of their agency's information security program for fiscal year 2025. OMB notes that level 4 (*managed and measurable*) represents an effective level of security.

enhance the agency's information security program. The agency further outlines actions to address each recommendation. In addition, we are closing three recommendations from our prior years' Federal Information Security Modernization Act of 2014 (FISMA) audit reports. Eight previously made recommendations in the areas of data loss prevention, data classification, flaw remediation, and system/software inventorying remain open. We will continue to monitor the CFPB's progress in addressing our open recommendations as part of future FISMA audits.

Recommendations, 2025-IT-C-012, October 31, 2025

2025 Audit of the CFPB's Information Security Program

Finding 1: Cybersecurity Risk Profiles Can Help the CFPB Assess, Tailor, and Prioritize Its Cybersecurity Approach

Number	Recommendation	Responsible office
1	Determine what ERM roles, responsibilities, and strategy components should be defined and leveraged for the development and maintenance of cybersecurity profiles.	Office of the Director
2	Develop and maintain cybersecurity risk registers to aggregate, normalize, and prioritize cybersecurity risks.	Operations Division and Office of Technology and Innovation
3	Develop policies and procedures to create and maintain cybersecurity profiles.	Operations Division and Office of Technology and Innovation

Finding 2: Maintaining System Authorizations Can Ensure That Risks to Sensitive Data Are Reduced

Number	Recommendation	Responsible office
4	Perform a review of previously granted RAMs 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 implement compensating controls as needed for affected systems.	Office of Technology and Innovation
5	Ensure that RAMs reflect an assessment of qualitative and quantitative cybersecurity risks, as applicable.	Office of Technology and Innovation
6	Evaluate options to perform ongoing information continuous monitoring activities commensurate with the current threat environment.	Office of Technology and Innovation

Contents

Introduction

Objectives

In accordance with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA), our audit objectives were to evaluate the effectiveness of the Consumer Financial Protection Bureau's (1) security controls and techniques for selected information systems and (2) 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 (FISMA) Reporting Metrics*.[2]

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) *Framework for Improving Critical Infrastructure Cybersecurity* (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 several metrics that IGs are required to assess using a maturity model.[4] Table 1 highlights the relationships between the function areas, the 10 security domains, and metrics.

In 2024, NIST updated the Cybersecurity Framework to include the *govern* function to underscore the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. This function consists of two

[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.

[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 U.S. Department of Homeland Security's 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. The total number of metrics IGs are required to assess declined from 37 for fiscal year 2024 to 25 for fiscal year 2025.

domains: cybersecurity governance and cybersecurity supply chain risk management.[5] *Govern* emphasizes organizational context; the establishment of cybersecurity strategy, roles, responsibilities, and authorities; cybersecurity supply chain risk oversight; and policy development. The *govern* function informs how an organization implements the other five functions, and as such, is a critical component for achieving and maintaining an effective information security program

Table 1. NIST Cybersecurity Framework Security Functions, Objectives, and Associated IG FISMA Reporting Domains

Security function	Security function objective	Associated IG FISMA reporting domain
Govern	Implement an understanding of organizational context; establish the cybersecurity strategy and cybersecurity supply chain risk management; define roles, responsibilities, and authorities; develop policy; and oversee the execution of cybersecurity strategy.	Cybersecurity governance (for example, oversight), cybersecurity supply chain risk management (for example, risk management strategy)
Identify	Develop an organizational understanding to manage cybersecurity risk to the agency assets and maintain a comprehensive and accurate inventory of system inventory and hardware, software, and data.	Risk and asset management (for example, risk assessment)
Protect	Implement safeguards to ensure delivery of critical infrastructure services as well as to prevent, limit, or contain the impact of a cybersecurity event.	Configuration management (for example, technology infrastructure resilience), identity and access management (for example, identity management, authentication, and access control), data protection and privacy (for example, data security), security training (for example, awareness and training)
Detect	Implement activities to identify the occurrence of cybersecurity events.	Information security continuous monitoring (for example, adverse event analysis)
Respond	Implement processes to take action regarding a detected cybersecurity event.	Incident response (for example, incident mitigation)
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	Contingency planning (for example, incident recovery plan execution)

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

[5] Office of Management and Budget, *FY 2025 IG FISMA Reporting Metrics*.

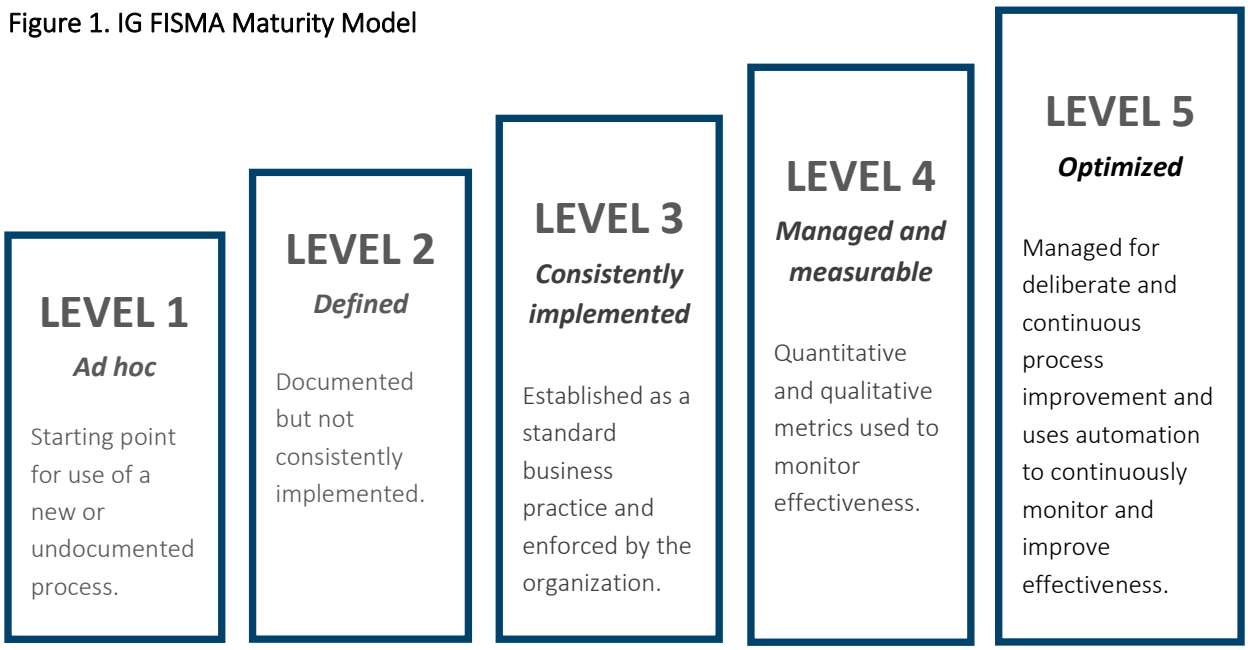
FISMA Maturity Model

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 (figure 1). 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.[6] Metric, domain, and function level maturity ratings factor into the overall determination of whether an agency's information security program is effective. Further details on the scoring methodology for the maturity model are included in appendix A.

Figure 1. IG FISMA Maturity Model



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

[6] 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*, Special Publication 800-53, Revision 5, updated December 10, 2020.

The CFPB's Information Security Program

Table 2 highlights key responsibilities that FISMA establishes for the agency head, chief information officer (CIO), and senior agency information security officer (SAISO) with respect to developing and maintaining an information security program.

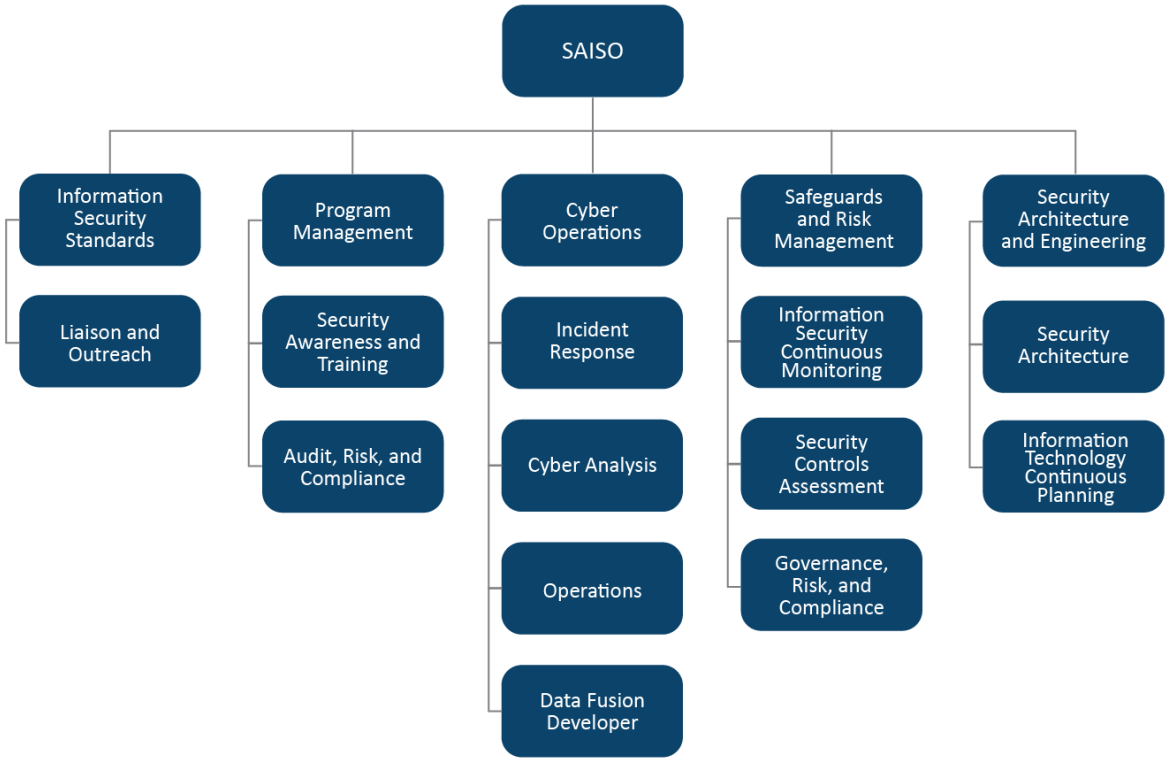
Table 2. Key FISMA Responsibilities for the Agency Head, CIO, and SAISO

Agency head	CIO	SAISO
• Provide information security protections for agency information and information systems commensurate with risk • Comply with FISMA requirements and related policies and standards • Ensure that information security management processes are integrated with agency strategic, operational, and budgetary planning processes • Ensure that senior agency officials provide information security for the information and systems under their control, including through periodic testing and evaluation of information security controls • Delegate to the CIO the authority to ensure compliance with FISMA requirements	Designate a SAISO who shall • Carry out the CIO's FISMA responsibilities • Head an office with the mission and resources to ensure agency compliance with FISMA • Possess professional qualifications, including training and experience required to administer FISMA requirements	Develop, document, and implement an information security program for the information and information systems that support the assets of the agency, including third-party systems, that includes • Periodic risk assessments • Risk-based policies and procedures that cost-effectively reduce risks to an acceptable level • Subordinate plans for providing adequate information security for networks, facilities, and systems • Security awareness training • Periodic testing and evaluation of the effectiveness of information security policies and procedures to include management, operational, and technical controls, for all agency information systems • Processes to remediate information security deficiencies • Procedures for detecting, reporting, and responding to security incidents • Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency

Source: OIG analysis based on Public Law 113-283.

To meet these responsibilities, the CFPB has established an information security program that resides within the agency's Office of Technology and Innovation, which is headed by the CIO. In accordance with FISMA, the CIO has delegated to the SAISO the authority to develop, document, and implement an information security program. The functional breakdown of the CFPB's information security program is provided in figure 2.

Figure 2. Functional Breakdown of the CFPB's Information Security Program



Source: OIG analysis.

To fulfill FISMA responsibilities, the CFPB has historically leveraged contractor resources to support its information security program. At the start of 2025, under a Blanket Purchase Agreement for IT security and compliance services provided via the Bureau of Fiscal Service, the CFPB had task orders in place for contractor support in the areas of cyber operations, information security continuous monitoring (ISCM), security controls testing, and program management activities. Of the approximately 65 individuals supporting the CFPB's information security program at the start of 2025, roughly 66 percent were contractors.

By the end of February 2025, roughly 25 percent of the remaining individuals supporting the program were contractors. This decrease resulted from task orders supporting ISCM, security controls testing, and program management activities being either terminated or de-obligated, resulting in the loss of contractor resources. Contractor support for cyber operations was kept. Along with staff departures, these actions have affected the ability of the agency to effectively maintain cybersecurity activities in those areas.

The CFPB continues to operate systems housing sensitive data. For example, in accordance with the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPB maintains systems to collect, investigate, and respond to consumer complaints and to supervise entities that provide consumers with financial products or services. These systems can contain personally identifiable information (PII), such as social security numbers, and confidential supervisory information (CSI). As such, we believe that the CFPB should continue to ensure adequate security is provided for these data and systems.

Summary of Audit Results of the CFPB's Information Security Program

The maturity of the CFPB's information security program has decreased from a level-4 maturity (*managed and measurable)* in fiscal year (FY) 2024 to a level-2 maturity (*defined*) in FY 2025. We further concluded, based on the results of our determinations of effectiveness in each domain and function, that the CFPB's overall information security program is not effective.[7] We identified three areas in which the CFPB should take steps to strengthen its information security program:

- Cybersecurity risk profiles. We found that the CFPB does not use cybersecurity profiles to assess, tailor, and prioritize its cybersecurity approach. A key contributing factor to this issue is a historical lack of maturity and governance to integrate cybersecurity and enterprise risk management activities.
- System authorization and continuous monitoring processes. We found that the CFPB is not consistently completing authorizations to operate (ATOs) or authorities to use (ATUs), instead using risk acceptance memorandums (RAMs), which do not properly document risks assessed. As noted previously, contributing factors include a loss of contractor support for the CFPB's ISCM efforts as well as a historical reliance on RAMs.
- End-of-life software. We found that the CFPB continues to use end-of-life software, which increases the risk of malicious actors bypassing security protections. A key reason for this issue is delays in modernizing, rearchitecting, and retiring legacy applications.

We also found that the CFPB has taken some steps to maintain and strengthen its information security program since our 2024 review. For example, the agency bolstered its incident response processes to address potential ransomware incidents. In addition, the CFPB took steps to strengthen personnel security processes by beginning enrollment in a continuous vetting process. Further, the SAISO continues to meet with system owners on a weekly basis to manage cybersecurity risks, and the agency is in the process of decommissioning and modernizing legacy technology systems.

Our report includes six new recommendations and one matter for management's consideration. Further, we are closing 3 of 11 recommendations from prior years' FISMA audit reports. These recommendations relate to security of the CFPB's governance, risk management and compliance tools, the reinvestigation of system users and personnel security, and the strengthening of processes to respond to potential ransomware incidents. The remaining 8 open recommendations are in the risk and asset management, configuration management, identity and access management, data protection and privacy, and contingency planning domains. Appendix B provides further details on the status of our prior years' FISMA audit recommendations.

[7] Appendix A explains the scoring methodology outlined in the *FY 2025 IG FISMA Reporting Metrics*, which we used to determine the maturity of the CFPB's information security program.

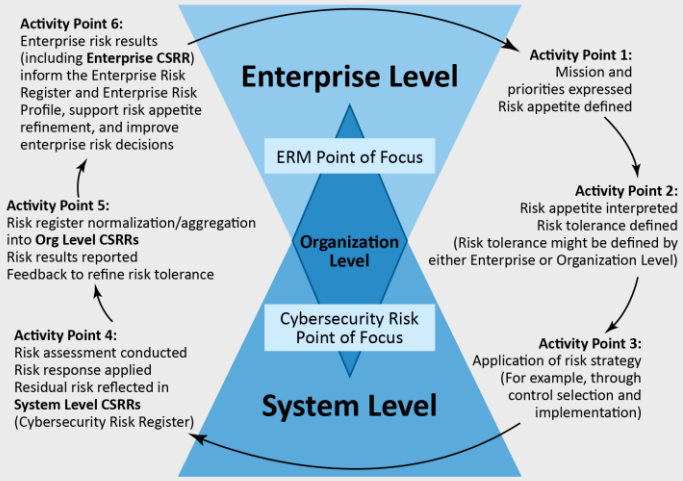
Finding 1: Cybersecurity Risk Profiles Can Help the CFPB Assess, Tailor, and Prioritize Its Cybersecurity Approach

A cybersecurity profile, consisting of a current profile and target profile, is used to help an organization identify its current and target cybersecurity posture by assessing information such as the organization's policies, risk management priorities, and cybersecurity requirements. The profile reflects an organization's mission objectives, stakeholder expectations, and threat landscapes. Organizations may use several cybersecurity profiles, which can be at different levels of the organization and for different types of information. For example, different divisions may develop their own cybersecurity profiles to address differences in data sensitivity, such as the handling of CSI or PII.

ERM AND THE CYBERSECURITY FRAMEWORK

An organization can get the most value out of the CSF, including the use of profiles, when it coordinates implementation activities with ERM. As shown below, an ERM program provides important information to guide the implementation of the CSF (activity point 1). Likewise, the CSF provides important information to the ERM program (activity point 6).

Figure 3. Illustration of Enterprise Risk and Coordination



Source: NIST publication IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*.

Although the CFPB has tailored information security controls and developed baselines, we found that the agency has not used cybersecurity profiles, or an alternative method, to establish and communicate its cybersecurity objectives and its approach to achieving its objectives, as well as to identify security gaps. While the agency completed a cybersecurity assessment containing an inherent risk profile and cybersecurity maturity assessment in 2021, that assessment does not contain the required elements of a current and target cybersecurity profile. Specifically, the assessment does not contain defined core cybersecurity risk management objectives that the agency is attempting to achieve, target outcomes the agency selected and prioritized, or anticipated changes to the agency's cybersecurity posture.

We identified four reasons affecting the CFPB's ability to develop and maintain cybersecurity profiles. First, as we have previously noted, the CFPB has historically not been effective in integrating

cybersecurity risk management and enterprise risk management activities.[8] Similarly, while the CFPB has a strategy to identify, assess, and manage risks at the system level, it does not have a strategy to guide and inform how security and privacy risks are framed, assessed, responded to, and monitored at the organizational level.[9] Secondly, this year we found that the CFPB does not use cyber security risk registers to aggregate, normalize, and prioritize cyber risks at an enterprise level.[10] As noted by NIST, these activities, along with risk management priorities, enterprise risk profiles, and work roles can help organizations effectively implement the Cybersecurity Framework (CSF) (see figure 3 above). Thirdly, the CFPB has not developed policies and procedures to develop and maintain current and target enterprise-wide cybersecurity profiles. Finally, this year we found that the CFPB's ERM program[11] has been placed on hold as the agency's chief risk officer and other individuals in the ERM office left the agency in March 2025. These individuals' positions have not been backfilled, nor are their roles and responsibilities being fully performed.

Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, issued in May 2017, requires agencies to follow the NIST Cybersecurity Framework to manage cybersecurity risk. According to CSF 2.0, organizations should develop and maintain a current cybersecurity profile that reflects mission objectives, threat landscape, and resources to guide implementation of cybersecurity activities.[12] Further, organizations should develop a target profile that specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management decisions. NIST further states that the CSF is most helpful to organizations when it is paired with ERM elements such as an understanding of what information and technology are most important to the enterprise mission and risk appetite and tolerance.[13]

The CFPB continues to operate systems housing sensitive data. For example, in accordance with the Dodd-Frank Act, the CFPB maintains systems to collect, investigate, and respond to consumer complaints and to supervise entities that provide consumers with financial products or services. These systems can contain PII, such as social security numbers, and CSI. Cybersecurity profile(s) can help ensure that cybersecurity protections and priorities are deployed commensurate with the threats faced by these systems.

[8] As part of our 2023 and 2024 responses to the IG FISMA metrics in CyberScope, we noted a lack of maturity in the CFPB's ability to integrate cybersecurity risk management and enterprise risk management processes, to include reporting, governance, and compliance activities.

[9] The *FY 2025 IG FISMA Reporting Metrics* include a new metric that asks IGs to determine the extent to which the organization uses a cybersecurity risk management strategy to support operational risk decisions, in accordance organizational priorities, constraints, risk appetite, and tolerance.

[10] In our 2021 FISMA audit report, we recommended that the CIO develop and implement a cybersecurity risk register and associated process to identify and manage organization-wide cybersecurity risks. In 2023, we closed this recommendation based on actions taken by the CIO. However, since then, the CFPB has not maintained its cybersecurity risk register.

[11] An enterprise risk management program enables agencies to aggregate, prioritize, and analyze risks from across the organization in a consistent format.

[12] The use of cybersecurity profiles is also outlined in CSF 1.1, dated April 2018.

[13] *Risk appetite* refers to the types and amount of risk, on a broad level, that an organization is willing to accept. *Risk tolerance* is the degree of risk or uncertainty that is acceptable to the organization.

Recommendations

We recommend that the acting CFPB director

1. Determine what ERM roles, responsibilities, and strategy components should be defined and leveraged for the development and maintenance of cybersecurity profiles.

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

2. Develop and maintain cybersecurity risk registers to aggregate, normalize, and prioritize cybersecurity risks.
3. Develop policies and procedures to create and maintain cybersecurity profiles.

Management Response

In response to the draft report, CFPB management concurs with our recommendations and notes that implementation of the recommendations will further enhance the agency's information security program. In response to recommendation 1, CFPB management states that the agency plans to update templates and further the development and maintenance of cybersecurity profiles. The CFPB expects to complete these updates by the fourth quarter of FY 2026. In response to recommendation 2, CFPB management states that the agency will work to enhance its existing tools to aggregate, normalize, and prioritize cybersecurity risks. The CFPB expects to complete these enhancements by the fourth quarter of FY 2026.

In response to recommendation 3, CFPB management states that the agency will incorporate new NIST requirements for cybersecurity risk profiles within its ERM framework. The CFPB expects to complete these updates by the fourth quarter of FY 2026.

OIG Comment

We believe that the actions described by CFPB management are responsive to our recommendations. We will follow up on the CFPB's actions to ensure that the recommendations are fully addressed.

In its management response, the CFPB states that our assertion that "the agency has not maintained cybersecurity risk registers" is misleading. The agency's response further notes that we closed a previous recommendation made in 2021 on developing and implementing a cybersecurity risk register and that NIST guidance in the area has not changed since. We agree that the CFPB took steps to strengthen its cybersecurity risk register process based on our 2021 recommendation. These steps resulted in us closing the recommendation in 2023. However, since then, NIST has issued several publications providing additional guidance on cybersecurity risk registers and their role in enterprise risk management. Our new recommendation reflects this new guidance.

Finding 2: Maintaining System Authorizations Can Ensure That Risks to Sensitive Data Are Reduced

As noted earlier, the CFPB continues to operate systems housing sensitive data, including PII, confidential investigative information, and CSI in support of requirements in the Dodd-Frank Act. The CFPB's information security policy, as well as federal requirements, requires systems to be authorized to operate before they are placed into production. Authorization involves an official management decision to accept the risk to systems based on an agreed-upon set of controls.[14] Once in operation, FISMA requires systems to be continuously monitored to provide ongoing awareness of their security posture, vulnerabilities, and threats. Organizations use ongoing authorizations[15] based on evidence produced from continuous monitoring programs to reduce the need for separate reauthorization processes. This helps ensure that cyber risk is managed efficiently and effectively.

We identified 35 CFPB systems that were operating with an expired ATO or ATU[16] or that never went through an authorization process. Fourteen systems were identified as operating with an expired ATO, and 21 systems were identified that used RAMs and did not go through the authorization process. We believe that this discrepancy is due to two key causes. First, the CFPB continues to use RAMs in lieu of ATOs or ATUs. The RAMs, however, were not based on a documented analysis of cybersecurity risks (quantitative or qualitative). Nineteen of 21 systems had RAMs that were signed before February 2025. Second, in February 2025, a termination for convenience was issued for the task order providing contractor resources for the CFPB's ISCM program. This action has resulted in a loss of contractor support. These resources have not been reinstated, and subsequently, government personnel supporting the program departed the agency. As such, the CFPB's ISCM program was not operational during significant portions of our fieldwork. However, CFPB officials informed us that they have since begun to identify resources to redeploy from other offices to perform ISCM functions.

NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, notes that risk acceptance decisions should be based on a complete review of the system or common controls. Further, the CFPB's *Risk Management Framework (RMF) Handbook* states that documentation regarding risk acceptances should include the risk/finding, criticality, reasoning why mitigation/transfer/avoidance cannot be met, and how long the risk will be approved.

Without current ATOs/ATUs and comprehensive RAMs, the CFPB does not have assurance that system security controls are operating effectively and risks have been mitigated to an acceptable level. Further,

[14] Per NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, system authorization decisions are supported by system security plans, assessment reports, and plans of actions and milestones.

[15] *Ongoing authorizations* refer to the continuous evaluation of the effectiveness of security and privacy control implementation.

[16] An authorization to use an information system, service, or application is based on the information in an existing authorization package generated by another organization.

the CFPB is unable to effectively perform ongoing assessments of security controls for its systems and supply chain partners.

Recommendations

We recommend that the CIO:

4. Perform a review of previously granted RAMs 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 implement compensating controls as needed for affected systems.
5. Ensure that RAMs reflect an assessment of qualitative and quantitative cybersecurity risks, as applicable.
6. Evaluate options to perform ongoing information continuous monitoring activities commensurate with the current threat environment.

Management Response

In response to the draft report, CFPB management concurs with our recommendations. In response to recommendation 4, CFPB management states that the agency will conduct an enterprise review of all active risk acceptances. The review will assess whether additional compensating controls or other countermeasures are required. The CFPB expects to complete these updates by the third quarter of FY 2026.

In response to recommendation 5, CFPB management states that the agency will evaluate and determine whether exceptions to the appropriate review and approval process are needed. For these exceptions, the CFPB will evaluate and update risk-based decisions based on qualitative and/or quantitative risks. The CFPB expects to complete these enhancements by the second quarter of FY 2026.

In response to recommendation 6, CFPB management states that the agency identified additional resources to assist with ISCM activities. In addition, the agency plans to issue a new task order for ISCM support in the second quarter of FY 2026. The CFPB expects to complete these updates by the fourth quarter of FY 2026.

OIG Comment

We believe that the actions described by CFPB management are responsive to our recommendations. We will follow up on the CFPB's actions to ensure that the recommendations are fully addressed.

In its management response, the CFPB notes that our report "provides the misleading impression that the Bureau has a lax information security posture. For example, the report states that the CFPB is not consistently completing authorizations to operate (ATOs) or authority to use (ATUs), instead using risk acceptance memorandums (RAMs), which do not properly document risks assessed." Further, the CFPB's response notes, "The report fails to mention that many of the systems are very low risk and do not contain any Bureau data." While we acknowledge that some systems may pose low risk to the

organization, a majority are classified as moderate within the system listing and there are others that include sensitive information, such as CSI and PII.

Further, CFPB management's response states that, with respect to using RAMs in lieu of ATOs and ATUs, "not once has the OIG questioned this practice or expressed concerns about it." We note, however, that in 2024 we communicated to senior CFPB leadership the concerns we have with the use of RAMs for the agency's evidence management system.

Matter for Management Consideration: Continued Use of End-of-Life Software Increases the Risk to Sensitive CFPB Data and Systems

The CFPB uses a variety of software programs to support functions ranging from the completion of day-to-day tasks to the maintenance and storage of PII, confidential investigative information, and CSI within systems. Vendors will typically discontinue support for a software program and stop developing, repairing, maintaining, and testing it when it reaches its end of life. Similarly, vendors may stop issuing security updates and patches for the software. In addition to enabling a bad actor to exploit security vulnerabilities, end-of-life software can introduce software compatibility issues.

We continue to identify instances of critical software platforms, along with software deployed to those platforms, that have reached their end of life and are no longer supported by vendors.[17] The CFPB has also identified these issues through its internal vulnerability scanning and remediation efforts. Further, CFPB officials informed us that they have not procured extended maintenance warranties[18] for end-of-life software, and we did not identify a risk acceptance on file.

BREACH RESULTING FROM END-OF-LIFE SOFTWARE

- In 2023, a federal agency was compromised by hackers who exploited vulnerabilities within end-of-life software. This exploit allowed for the hackers to steal user credentials and move laterally within the network.
- While damages were limited, threat actors were able to deploy additional malware to the agency before discovery.

In 2024, we issued a restricted, early alert memorandum to the CFPB highlighting the security risk posed by using end-of-life software.[19] In that memorandum, we highlighted a software product that would be reaching its end of life in 2024. This software has since reached its end of life and continues to be operated by the CFPB. While the CFPB is taking steps to remediate some end-of-life software, its efforts are hindered by the need to replatform, retire, and/or modernize applications and migrate them fully to the cloud.

[17] Because of the sensitivity of these issues, we communicated the details to CFPB officials separately.

[18] Software vendors can offer extended warranties that provide content and security updates to customers using software that has reached its end of life.

[19] Office of Inspector General, *OIG Early Alert Memorandum Report: The Use of End-of-Life Critical Software Increases the CFPB's Exposure to Potential Vulnerabilities*, May 20, 2024.

In addition, our 2024 FISMA audit report includes an open recommendation for the CIO to 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.[20] This recommendation also covers the vulnerabilities posed by end-of-life software. By ensuring that software is upgraded to a supported version in a timely manner, the CFPB can reduce the risk from potential vulnerabilities for which no fixes are available from the vendor. We believe that CFPB management should prioritize efforts to migrate end-of-life software to vendor-supported versions.

Because our 2024 FISMA recommendation remains open, we do not include a new recommendation but suggest that management prioritize efforts to address the open recommendation and reduce the risks resulting from the use of outdated software.

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

Appendix A: Scope and Methodology

Our specific audit objectives, based on FISMA requirements, 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. To accomplish our objectives, we reviewed the effectiveness of the CFPB 's information security program across the six function areas outlined in the *FY 2025 IG FISMA Reporting Metrics*.

To assess the effectiveness of the CFPB's information security program, we

- focused our detailed testing activities on the annual core metrics and supplemental FY 2025 metrics identified in the *FY 2025 IG FISMA Reporting Metrics*[21]
- analyzed security policies, procedures, and documentation
- interviewed CFPB management and staff
- observed and tested specific security processes and controls at the program and information system level for three sampled CFPB systems [22]

To determine whether the CFPB's information security program is effective, we used the scoring methodology defined in the *FY 2025 IG FISMA Reporting Metrics*. Specifically, the metrics note that IGs have the discretion to determine whether an agency is effective in each of the CSF functions and whether the agency's overall information security program is effective based on the results of the determinations of effectiveness in each domain, function, and overall program assessment. The metrics also direct IGs to place greater emphasis on the core metric ratings and use the supplemental metrics scores as part of their risk-based determinations of effectiveness.

In accordance with this methodology, we determined maturity ratings at the cybersecurity function and domain levels and factored in our knowledge of the CFPB's risk environment to come to our conclusions. We entered our specific maturity ratings at the function and domain levels in the CyberScope FISMA reporting application.

We conducted this work from April 2025 to October 2025. 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.

[21] Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness. Supplemental metrics are not considered a core metric but represent important activities conducted by security programs and contribute to the overall determination of security program effectiveness.

[22] To select these three systems, we used a risk-based methodology that included consideration of system risk levels, data types, technologies, users, and previously completed OIG work. We plan to communicate the results for these systems to the CFPB separately.

Appendix B: Status of Prior FISMA Recommendations

Table B-1. Status of Prior FISMA Recommendations That Were Open as of the Start of Our Fieldwork, by Security Domain

Year		Recommendation	Status	Explanation
Risk management				
2022	4	We recommend that the CIO ensure that an enterprise-wide software inventory is conducted and maintained.	Open	The CFPB is in the process of completing an enterprise-wide software inventory.
2024	7	We recommend that the CIO renew the ATU for the CFPB's governance, risk, and compliance (GRC) tool.	Closed	The CFPB renewed its ATU for its GRC tool on April 1, 2025.
2024	8	We recommend that the CIO implement a process that ensures the cyber risk information in the CFPB's GRC tool is accurate and maintained.	Open	We continue to identify inaccuracies in the ATO and ATU status of systems maintained in the CFPB's GRC tool and have communicated the details to the CFPB separately.
Configuration management				
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	CFPB officials notified us that they have begun to work on corrective actions, which should be completed by the first quarter of FY 2026.
Identity and access management				
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.	Open	CFPB officials notified us that because of resource constraints, the agency has not fully implemented its automated privileged user access management process in its identity and access management tool.

Year		Recommendation	Status	Explanation
2024	4	We recommend that the chief administrative officer ensure that adequate resources are allocated to reinvestigate CFPB systems users as required.	Closed	The CFPB established a memorandum of understanding with the Defense Counterintelligence and Security Agency for its participation in a continuous vetting process, replacing the legacy 5-year periodic reinvestigation. The CFPB has enrolled 87 percent of eligible federal staff and contractors into the first phase of the program as part of this continuous vetting process.
Data protection and privacy				
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	While the CFPB has drafted an agencywide data classification policy that accounts for the sensitivity of the data maintained by the CFPB, the policy has not been finalized.
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.
Incident response				
2024	5	We recommend that the CIO develop and maintain a ransomware strategy and specific procedures that provide a formal, focused, and coordinated approach to responding to ransomware attacks.	Closed	The CFPB has developed a ransomware strategy and procedures to help provide a coordinated approach to responding to ransomware attacks.

Year		Recommendation	Status	Explanation
Contingency planning				
2023	1	We recommend that the CIO, in coordination with business and mission stakeholders, perform the following steps for relevant systems: • Maintain a comprehensive schedule for testing and exercising the current contingency plans. • Document test procedures. • Create relevant updates to the plan to improve the CFPB's resilience.	Open	The CFPB is in the process of implementing a comprehensive schedule for testing and exercising the current contingency plans.
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 has not yet tested the mission-essential functions identified in the continuity of operations plan.

Source: OIG analysis.

Appendix C: Management Response

Consumer Financial Protection Bureau

1700 G Street NW, Washington, D.C. 20552

October 30, 2025

Mr. Khalid Hasan
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. Hasan,

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the *2025 Audit of the CFPB's Information Security Program.* We acknowledge that you found the Consumer Financial Protection Bureau's (CFPB) Information Security Program is a level 2 (*defined*) maturity based on the Federal Information Security Modernization Act of 2014 (FISMA) maturity model.[1] The Bureau would like to correct the record because the report lacks crucial context.

First, the OIG's report provides the misleading impression that the Bureau has a lax information security posture. For example, the report states that "the CFPB is not consistently completing authorizations to operate (ATOs) or authority to use (ATUs), instead using risk acceptance memorandums (RAMs), which do not properly document risks assessed." Report at 12. As the OIG is aware, the Bureau has been using RAMs in lieu of ATOs and ATUs in certain instances for many years. Not once has the OIG questioned this practice or expressed concerns about it. Instead, the report implies the OIG has uncovered a serious issue because it identified 21 "systems" where the Bureau used a RAM in lieu of an ATO or ATU. The report fails to mention

[1] To be sure, the majority of federal agencies have received similar overall ratings. Office of Management & Budget, Federal Information Security Modernization Act of 2014 Annual Report Fiscal Year 2023 at 16.

consumerfinance.gov

that many of these "systems" are very low risk and do not contain any Bureau data. In fact, these 21 "systems" include subscriptions like WestLaw and LexisNexis, and even systems managed by other Federal agencies like the Federal Trade Commission's Consumer Sentinel and the Financial Crimes Enforcement Network Portal.

Second, the OIG's report claims that this year the OIG "found that the CFPB does not use cyber security risk registers to aggregate, normalize, and prioritize cyber risks at an enterprise level." Report at 14. The report goes on to claim that the OIG previously identified this issue in 2021 and closed an associated recommendation in 2023 "based on actions taken by the CIO," but that the "CFPB has not maintained its cybersecurity risk register." Report at 14, FN 9. This is misleading. In response to the OIG's 2021 recommendation, the Bureau created its Chief Risk Officer (CRO) Library. In 2023, the OIG determined that the CRO Library was sufficient to close this recommendation. Now, although the CFPB still maintains its CRO Library, the OIG no longer considers it adequate despite the fact that NIST publication IR 8286A – providing guidance concerning cybersecurity risk registers – has not been updated since 2021 when the OIG issued its pervious recommendation. Instead of acknowledging that it is moving the goal posts, the OIG claims it recently "found" something it has known about for two years.

I would also like to highlight some of the many steps the Bureau took in FY 2025 to improve its cybersecurity posture. In December 2024, the Bureau fully implemented Zscaler, which was a major improvement to our Zero Trust Architecture. The Zscaler solutions that have been implemented reduce both the likelihood and significance of a cybersecurity breach. The Bureau decommissioned 19 legacy systems or subsystems. This work has simplified the Bureau's infrastructure and mitigated cybersecurity risks. We closed 45% of open Plan of Action and Milestones (POAMs) related to security vulnerabilities and migrated the CFPB website to a significantly more secure cloud environment. We also implemented enhanced cybersecurity tools for log management and software composition analysis and increased the number of applications leveraging phishing resistant multifactor authentication by 19%.

This work demonstrates the Bureau's commitment to ensuring it has a robust cybersecurity posture. Notably, the Bureau did not have any major information security incidents or breaches of personally identifiable information in 2025.

In sum, although the Bureau generally concurs with the OIG's recommendations, the Bureau believes many of them represent non-material issues and documentation updates with little practical impact on the Bureau's cybersecurity posture. The Bureau will continue to focus its effort and resources on actions that have a real-world impact on the security of its systems.

Thank you for the professionalism and courtesy that you and all the OIG personnel showed throughout this review. We appreciate the OIG for noting CFPB's progress on remediating recommendations from previous audits. Our responses to the cited recommendation are below.

Sincerely,

CHRISTOPHER CHILBERT Digitally signed by CHRISTOPHER CHILBERT
Date: 2025.10.30 12:17:13 -04'00'

Christopher Chilbert
Chief Information Officer

Response to recommendations presented in the OIG Draft Report: ***2025 Audit of the CFPB's Information Security Program***

Recommendation 1: Determine what enterprise risk management roles, responsibilities, and strategy components should be defined and leveraged for the development and maintenance of cybersecurity profiles.

Management Response:

Despite the concerns expressed in the CFPB's response letter, the CFPB concurs that this recommendation will further enhance its information security program. CFPB currently has existing management roles and responsibilities defined and operated through two governing bodies (the Enterprise Risk Committee (ERC) and the Enterprise Risk Monitoring Council (ERMC)) as well as a process framework for how risks are identified and managed on risk profiles. CFPB will update these templates and plans to further the development and maintenance of cybersecurity risk profiles to reflect new NIST requirements. We expect to complete these updates by FY2026 Q4.

Recommendation 2: Develop and maintain cybersecurity risk registers to aggregate, normalize, and prioritize cybersecurity risks.

Management Response:

Despite the concerns expressed in the CFPB's response letter, the CFPB concurs that this recommendation will further enhance its information security program. CFPB will work to enhance its existing CRO Library to aggregate, normalize, and prioritize cybersecurity risks within the enterprise risk management framework. Further, the tool will be updated to enable a response and notification process to applicable risk owners in accordance with NIST requirements. We expect to complete these updates by FY2026 Q4.

Recommendation 3: Develop policies and procedures to create and maintain cybersecurity profiles.

Management Response:

Despite the concerns expressed in the CFPB's response letter, the CFPB concurs that this recommendation will further enhance its information security program. The CFPB currently has risk profiles and identified risk owners that are updated once per fiscal year. The CFPB will incorporate the new NIST requirements for cybersecurity's risk profile to be included in the

enterprise risk management framework and update existing templates and procedures to reflect the new requirements for risk profiles. We expect to complete these updates by FY2026 Q4.

Recommendation 4: Perform a review of previously granted RAMs 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.

Management Response:

Despite the concerns expressed in the CFPB's response letter, the CFPB concurs that this recommendation will further enhance its information security program. The CFPB will conduct an enterprise review of all active risk acceptances in CSAM/JCAM. First, the CFPB will verify if each associated system remains in use; if not, it will be decommissioned in accordance with the Bureau's information system decommission process and related risk acceptances will be closed.

For systems that are confirmed in use, remediation actions will be prioritized through project governance, and each risk acceptance will complete an Authority to Operate (ATO) or Authority to Use (ATU) process for Authorizing Official decision-making, either as an update to an existing ATO if the application resides within an established system boundary, or a full ATO, as required. This review will assess whether these systems require additional compensating controls or other countermeasures based on the current threat landscapes and system configurations. POA&Ms will also be captured for any weaknesses identified. We expect to complete this review and associated updates by FY2026 Q3.

Recommendation 5: Ensure that risk acceptances reflect an assessment of qualitative and quantitative risks.

Management Response:

Despite the concerns expressed in the CFPB's response letter, the CFPB concurs that this recommendation will further enhance its information security program. Going forward, the CFPB will inform all system and service owners that any system or application intended for production use must complete the appropriate review and approval process (e.g., standard/non-standard software review, ATO, ATU, IATO). Exceptions requiring only a risk-based determination drafted for Authorizing Official (AO) approval will be permitted on per-control basis. For these exceptions, the CFPB will evaluate and update this risk-based decision to include an assessment approach for either qualitative and/or quantitative risks. We expect to complete this review and associated updates by FY2026 Q2.

Recommendation 6: Evaluate options to perform ongoing information continuous monitoring activities commensurate with the current threat environment.

Management Response:

Despite the concerns expressed in the CFPB's response letter, the CFPB concurs that this recommendation will further enhance its information security program. The CFPB has identified three individuals to assist with resourcing the information system continuous monitoring (ISCM) program. These resources are on loan, and as such the ISCM program will leverage these individuals with an automated Compliance System Continuous Monitoring feature. These trainees will begin ISCM assessments on authorized systems in accordance with the approved ISCM quarterly and annual assessment schedule. Additionally, the CFPB will update its ISCM process document to further define CFPB's "Frequency based" assessment procedures. Finally, CFPB is issuing a new task order for ISCM support that is expected to be awarded in FY2026 Q2. We expect to complete make the applicable updates to procedures by FY2026 Q4.

Abbreviations

ATO	authority to operate
ATU	authorization to use
CIO	chief information officer
CSF	Cybersecurity Framework
CSI	confidential supervisory information
Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*
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
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	personally identifiable information
RAM	risk acceptance memorandum
RMF	Risk Management Framework
SAISO	senior agency information security officer

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

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 Information

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