

Consumer Financial Protection Bureau

2024 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, 2024-IT-C-019, October 31, 2024

2024 Audit of the CFPB's Information Security Program

Findings

The Consumer Financial Protection Bureau's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. We found that the CFPB has taken several steps to strengthen its information security program since our 2023 Federal Information Security Modernization Act of 2014 (FISMA) review. For instance, the CFPB improved its security training program by incorporating threat intelligence to update its workforce on a near-real-time basis.

To ensure that its information security program remains effective, the agency can

- mature data loss prevention (DLP) processes by developing data classification policies and procedures and by configuring its DLP tool accordingly
- strengthen processes to ensure timely remediation of critical and high-risk vulnerabilities
- ensure that system users are periodically reinvestigated to maintain access authorizations and privileges
- improve incident processes to effectively respond to a potential ransomware incident
- strengthen organizational resiliency by conducting a comprehensive test of its continuity of operations plan
- ensure the accuracy of the information in its cybersecurity governance, risk, and compliance tool

In addition, of the seven open recommendations made in our prior years' FISMA audit reports, the CFPB has taken sufficient actions to close four. We will continue to monitor the CFPB's progress in addressing our open recommendations as part of future FISMA audits.

Recommendations

This report includes eight new recommendations designed to strengthen the CFPB's information security program in the areas of DLP, vulnerability management, personnel security, incident management, contingency planning, and risk management. In its response to a draft of our report, the CFPB concurs with our recommendations and outlines actions to address each recommendation. We will monitor the CFPB's progress in addressing these recommendations as part of future FISMA audits.

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 2023–2024 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 2024. OMB notes that level 4 (*managed and measurable*) represents an effective level of security.



Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Recommendations, 2024-IT-C-019, October 31, 2024

2024 Audit of the CFPB's Information Security Program

Finding 1: Improving DLP Processes Can Better Protect Sensitive Data

Number	Recommendation	Responsible office
1	Complete finalization of an agencywide data classification policy that accounts for the sensitivity of the data maintained by the CFPB.	Office of the Chief Data Officer
2	Ensure that data classification and sensitivity labels are incorporated into the CFPB's DLP program.	Office of Technology and Innovation

Finding 2: Timely Mitigation of Technical Vulnerabilities Can Reduce the Attack Surface

Number	Recommendation	Responsible office
3	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.	Office of Technology and Innovation

Finding 3: Conducting Periodic Reinvestigations of System Users Can Help Protect Against Insider Threats

Number	Recommendation	Responsible office
4	Ensure that adequate resources are allocated to reinvestigate CFPB systems users as required.	Office of Administrative Operations

Finding 4: Strengthening Incident Response Processes Can Ensure Effective Responses to Ransomware Incidents

Number	Recommendation	Responsible office
5	Develop and maintain a ransomware strategy and specific procedures that provide a formal, focused, and coordinated approach to responding to ransomware attacks.	Office of Technology and Innovation

Finding 5: Comprehensive COOP Testing Can Help Improve Organizational Resiliency

Number	Recommendation	Responsible office
6	Ensure that testing of mission-essential functions identified in the CFPB's COOP is periodically performed.	Office of Administrative Operations

Finding 6: Ensuring Accurate Risk Information in the Cybersecurity GRC Tool Can Help Prioritize Risk Responses

Number	Recommendation	Responsible office
7	Renew the ATU for the CFPB's GRC tool.	Office of Technology and Innovation
8	Implement a process that ensures the cyber risk information in the CFPB's GRC tool is accurate and maintained.	Office of Technology and Innovation



Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: October 31, 2024

TO: Distribution List

FROM: Khalid Hasan 
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2024-IT-C-019: *2024 Audit of the CFPB's Information Security Program*

We have completed our report on the subject audit. We performed this audit pursuant to requirements in the Federal Information Security Modernization Act of 2014 (FISMA). Specifically, FISMA requires each agency inspector general to conduct an annual independent evaluation of the effectiveness of their agency's information security program and practices. As part of our work, we also reviewed security controls for selected agency systems and performed other technical tests. We plan to transmit the detailed results of this testing in separate memorandums. In addition, we used the results of this audit to respond to specific questions in the Office of Management and Budget's *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

We provided you with a draft of our report for your review and comment. In your response, you concur with our recommendations and outline actions that have been or will be taken to address our recommendations. We have included your response as appendix C to our report.

We appreciate the cooperation that we received from CFPB personnel during our review. Please contact me if you would like to discuss this report or any related issues.

cc: Jan Singelmann
Adam Martinez
Jean Chang
Irfan Malik
Tiina Rodrigue
Marianne Roth
Richard Austin
Ashley Adair

Distribution:

Chris Chilbert, Chief Information Officer
Martin Michalosky, Chief Administrative Officer
Ren Essene, Chief Data Officer



Contents

Introduction	8
Objectives	8
Background	8
FISMA Maturity Model	9
Summary of the CFPB’s Information Security Program	10
Finding 1: Improving DLP Processes Can Better Protect Sensitive Data	12
Recommendations	13
Management Response	13
OIG Comment	13
Finding 2: Timely Mitigation of Technical Vulnerabilities Can Reduce the Attack Surface	14
Recommendation	14
Management Response	15
OIG Comment	15
Finding 3: Conducting Periodic Reinvestigations of System Users Can Help Protect Against Insider Threats	16
Recommendation	16
Management Response	16
OIG Comment	17
Finding 4: Strengthening Incident Response Processes Can Ensure Effective Responses to Ransomware Incidents	18
Recommendation	18
Management Response	18
OIG Comment	19
Finding 5: Comprehensive COOP Testing Can Help Improve Organizational Resiliency	20
Recommendation	21
Management Response	21
OIG Comment	21

Finding 6: Ensuring Accurate Risk Information in the Cybersecurity GRC Tool Can Help Prioritize Risk Responses	22
Recommendations	24
Management Response	24
OIG Comment	24
Appendix A: Scope and Methodology	25
Appendix B: Status of Prior FISMA Recommendations	26
Appendix C: Management Response	28
Abbreviations	34



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) 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 2023–2024 Inspector General Federal Information Security Modernization Act (FISMA) Reporting Metrics*.

The IG FISMA reporting metrics are grouped into nine security domains, which align with the five function areas in the National Institute of Standards and Technology’s (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework). These five function areas are *identify, protect, detect, respond, and recover* (table 1).² 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.³

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 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.

³ As noted in the *FY 2023–2024 IG FISMA Reporting Metrics*, IGs should use the U.S. Department of Homeland Security’s CyberScope application to submit the results of their metrics evaluation, to include maturity level ratings. As such, our detailed responses and assessment of the CFPB’s progress in implementing these metrics were provided in the CyberScope application. Because of the sensitive nature of our responses, they are restricted and not included in this report.

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

Security function	Security function objective	Associated IG FISMA reporting domain
<i>Identify</i>	Develop an organizational understanding to manage cybersecurity risk to agency assets.	Risk management, supply chain risk management
<i>Protect</i>	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, identity and access management, data protection and privacy, security training
<i>Detect</i>	Implement activities to identify the occurrence of cybersecurity events.	Information security continuous monitoring
<i>Respond</i>	Implement processes to take action regarding a detected cybersecurity event.	Incident response
<i>Recover</i>	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	Contingency planning

Source: U.S. Department of Homeland Security, *FY 2023–2024 Inspector General Federal Information Security Modernization Act (FISMA) Reporting Metrics*, Version 1.1, February 10, 2023.

FISMA Maturity Model

The five levels of the maturity model are

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 2023–2024 IG FISMA Reporting Metrics*, within the context of the maturity model, OMB believes that achieving a level 4 (*managed and measurable*) or above represents an effective level of security.⁴ Further details on the scoring methodology for the maturity model are included in appendix A.

⁴ 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.



Summary of the CFPB's Information Security Program

The CFPB's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity.⁵ We found that the CFPB has taken several steps to strengthen its information security program since our 2023 FISMA review. For instance, the CFPB has updated its enterprise business impact analysis (BIA) and ensured that the results are used to make applicable changes to related contingency and continuity plans. In addition, the CFPB has strengthened its security training program by incorporating threat intelligence to update its workforce on a near-real-time basis, resulting in the agency's first level-5 (*optimized*) maturity rating for a FISMA metric.

This report includes eight new recommendations designed to strengthen the CFPB's information security program in the areas of data loss prevention (DLP), vulnerability remediation, personnel security, incident response, continuity of operations, and cybersecurity risk management. In addition, of the seven open recommendations made in our prior years' FISMA audit reports, the CFPB has taken sufficient actions to close four; they are related to the development of policies and procedures for an enterprise software inventory and the maintenance of an enterprise BIA. The three remaining open recommendations relate to software asset management, contingency plan testing, and privileged access management. Appendix B provides further details on the status of our prior years' recommendations.

We identified opportunities for the CFPB to mature its information security program in the following areas:

- **DLP.** We found that while the CFPB has strengthened its DLP processes, it has not finalized a data classification policy that defines sensitivity labels. Data classifications and sensitivity labels can enable the agency to effectively detect and prevent the potential unauthorized exfiltration of sensitive information.
- **Vulnerability remediation.** The CFPB has established a vulnerability scanning program and is tracking remediation activities; however, we continue to find that the agency has not ensured that critical and high-risk system vulnerabilities in its information technology systems are timely remediated. Timely remediation of vulnerabilities can assist the CFPB in reducing its attack surface.⁶
- **Personnel security.** We found that the CFPB did not ensure that system users were periodically rescreened as a condition for maintaining access authorizations and privileges. While initial background screening processes are operating as intended, ensuring that periodic reinvestigations are performed can help reduce insider threat risk.

⁵ Appendix A explains the scoring methodology outlined in the *FY 2023–2024 IG FISMA Reporting Metrics*, which we used to determine the maturity of the CFPB's information security program.

⁶ According to NIST, an entity's *attack surface* is the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from that system, system element, or environment.

- **Incident response.** The CFPB has developed strategies, policies, and procedures to respond to various cybersecurity incidents; however, these do not specifically cover ransomware. Updating strategies, policies, and procedures to incorporate ransomware can strengthen organizational resiliency.
- **Continuity of operations.** We found that while the CFPB has updated its BIA and continuity of operations plan (COOP), the plan has not been fully tested. Testing the plan can help to ensure organizational resiliency.
- **Cybersecurity risk management.** The CFPB has implemented a cybersecurity governance, risk, and compliance (GRC) tool to help standardize and centralize processes. We found instances of inaccurate information in the tool. Ensuring accurate information in the cybersecurity GRC tool can help with management decisionmaking and effective resource prioritization.



Finding 1: Improving DLP Processes Can Better Protect Sensitive Data

Data classification is the process an organization uses to characterize its data assets using consistent labels so those assets can be managed properly. Data classification is vital for protecting an organization's data at scale because it enables the application of cybersecurity and privacy protection requirements to the organization's data assets. Data classification policies and DLP tools work together to protect sensitive data by classifying data, using classifications to create DLP policies, and enforcing actions.

To protect against the unauthorized exfiltration of sensitive agency information, among other things, the CFPB has implemented a network-based organizational DLP tool and developed a DLP policy and procedures. The agency has also strengthened DLP processes and configurations to account for a changing threat environment. However, we found that the CFPB's DLP tool is not effectively configured to prevent the disclosure of sensitive information.⁷ The reason for this is that the agency has not finalized its data classification policy that defines sensitivity labels. Data classifications and sensitivity labels can be used to effectively configure the agency's DLP tool and related processes.

NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, requires that organizations develop, document, and disseminate policies and procedures to facilitate the implementation of DLP controls. In addition, NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, notes that organizations can employ automated tools, such as DLP technologies, to monitor personally identifiable information internally or at network boundaries for unusual or suspicious transfers or events. Further, OMB Memorandum 22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, emphasizes that security and data teams should work together to develop data category and security rules to automatically detect and ultimately block unauthorized access to sensitive information.

The DLP system is not effectively configured because the CFPB has not finalized a data classification policy. In 2023, the CFPB updated its *Information Governance Policy*, which references processes for the proper intake, management, disclosure, and disposition of information. However, the policy does not align with the classifications established in FISMA and does not cover the full spectrum of information handled at the CFPB. CFPB officials informed us that they are working with the National Archives and Records Administration and OMB to finalize agency-specific data classifications, which will then be incorporated into a formal data classification policy; the agency has drafted, and expects to issue, the policy by the end of calendar year 2024. We believe that effective DLP processes are critical to preventing and detecting potential unauthorized exfiltration of information.

⁷ Because of the sensitivity of these issues, we communicated the details to CFPB officials separately .

Recommendations

We recommend that the chief data officer

1. Complete finalization of an agencywide data classification policy that accounts for the sensitivity of the data maintained by the CFPB.

We recommend that the chief information officer (CIO)

2. Ensure that data classification and sensitivity labels are incorporated into the CFPB's DLP program.

Management Response

CFPB management concurs with our recommendations. In response to recommendation 1, CFPB management states that the CFPB has taken steps to develop and implement a controlled unclassified information (CUI) program, including drafting a CUI policy that outlines roles and responsibilities and identifies 13 categories of CUI. The CFPB expects to complete the CUI policy by the fourth quarter of fiscal year 2025.

In response to recommendation 2, CFPB management states that the CFPB has aligned the DLP rules with the draft CUI policy and is prepared to make updates as the policy is finalized. The CFPB expects to complete these updates by the first quarter of fiscal year 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.



Finding 2: Timely Mitigation of Technical Vulnerabilities Can Reduce the Attack Surface

The CFPB's vulnerability management program is an essential component of its information security program because it enables the CFPB to reduce the agency's attack surface. The CFPB performs routine automated vulnerability and compliance scans to detect vulnerabilities and noncompliant configurations on CFPB information technology assets. However, we found numerous critical and high-risk operating systems and application vulnerabilities that were identified in the CFPB's internal vulnerability scans but were not timely remediated.⁸

The CFPB's *Vulnerability Management Process—Standard Operating Procedure* establishes requirements for the timely remediation of critical and high-risk vulnerabilities. Further, NIST Special Publication 800-53, Revision 5, requires that organizations install security-relevant software and firmware updates within an organization-defined period of the release of the updates.

These issues exist because the agency does not clearly map affected systems and their associated system owners in its configuration management database. A CFPB official also informed us that the agency uses broad categories in its configuration management database tool to group vulnerabilities, making it difficult to effectively manage the timely remediation of vulnerabilities. Timely remediation of critical and high-risk vulnerabilities will help reduce the CFPB's attack surface.

We previously reported on the need to strengthen technical configuration management process. Specifically, our 2018 FISMA report includes a recommendation for the CIO to strengthen configuration management processes by (1) remediating configuration-related vulnerabilities in a timely manner and (2) ensuring that optimal resources are allocated to perform vulnerability remediation activities.⁹ We are closing this recommendation and making a new recommendation that we believe will better enable the CFPB to address root causes related to untimely remediation of technical vulnerabilities.

Recommendation

We recommend that the CIO

3. 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.

⁸ Because of the sensitivity of these issues, we communicated the details to CFPB officials separately. We also issued a restricted early alert memorandum related to this issue in May 2024.

⁹ Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, [OIG Report 2018-IT-C-018](#), October 31, 2018.

Management Response

CFPB management concurs with our recommendation. In the response, CFPB management states that the agency will address a portion of this recommendation by integrating additional data sources into its configuration management database and ensuring the accurate mapping of those sources. In addition, management notes that the CFPB has initiated an automated process and program to identify, review, and report on operating system and application vulnerabilities. The CFPB expects to complete these updates by the fourth quarter of fiscal year 2026.

OIG Comment

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



Finding 3: Conducting Periodic Reinvestigations of System Users Can Help Protect Against Insider Threats

We found multiple users of sampled CFPB systems who have not been reinvestigated after 5 years as required, resulting in an increased insider threat risk. The sampled systems include those that process, store, or maintain sensitive information, including personally identifiable and confidential supervisory information.

The CFPB's personnel security policy establishes principles that ensure that federal employees and contractors are suitable for government employment. Specifically, the policy notes that periodic reinvestigations of all employees and contractors helps to ensure that these individuals continue to meet suitability requirements and that their employment or conduct will not jeopardize the efficiency of the civil service or pose a risk to national security, public safety, or the agency, including reputational harm, loss of data, or an adverse effect on consumers. Further, the policy states that all persons employed by or seeking employment with the CFPB, or those who perform work for or on behalf of the CFPB (for example, contractors), are required to undergo an initial background investigation and reinvestigation every 5 years.

CFPB officials have indicated that they do not have sufficient resources to perform all required reinvestigations and have prioritized the screening of new staff to help meet mission requirements. Further, CFPB officials noted that the Defense Counterintelligence and Security Agency and the Office of Personnel Management, which the agency relies on to conduct reinvestigations, have experienced processing delays. Ensuring that users' continued access to systems is contingent on a favorable reinvestigation can better protect against insider threats.

Recommendation

We recommend that the chief administrative officer (CAO)

4. Ensure that adequate resources are allocated to reinvestigate CFPB systems users as required.

Management Response

CFPB management concurs with our recommendation and notes that reinvestigations have been delayed by approximately 1 year because of competing priorities. Additionally, management notes that the nature of the background investigation process and reliance on other agencies increases the potential for delays. Further, management states that the agency has prioritized the completion reinvestigation backlogs and expects to have them completed by the fourth quarter of fiscal year 2026.

OIG Comment

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



Finding 4: Strengthening Incident Response Processes Can Ensure Effective Responses to Ransomware Incidents

Ransomware is a form of malware designed to encrypt files on a device, rendering them and the systems that rely on them unusable until a decryption key is provided. Ransomware incidents can severely affect business processes by leaving organizations unable to access necessary data to operate and deliver mission-critical services. As reported in Verizon's *2023 Data Breach Investigations Report*, ransomware continues to be a major threat for organizations of all sizes and industries and is present in 24 percent of breaches.¹⁰ Further, according to Federal Bureau of Investigation's *2023 Internet Crime Report*, government facilities were the third-largest critical infrastructure sector targeted by ransomware attacks.¹¹ We found that the CFPB does not have a ransomware strategy or procedures that include specific actions to be taken in the event of a ransomware attack on CFPB systems.

NIST Special Publication 800-53, Revision 5, requires organizations to develop guidelines related to incident handling, monitoring, and reporting. In addition, the Cybersecurity and Infrastructure Security Agency has issued the *#StopRansomware Guide* to combat the increased number of ransomware attacks affecting federal agencies.¹² The guide includes industry best practices and a response checklist that can serve as an addendum to an organization's cybersecurity incident response plans specific to ransomware.

CFPB officials informed us that they rely on their overarching incident response plan for ransomware incidents. However, this plan does not cover specific actions to be taken in the event of a ransomware incident. Although we are not aware of any ransomware attacks on the CFPB, the rising prevalence of such attacks highlights the need for the CFPB to formalize its strategy and processes in this area.

Recommendation

We recommend that the CIO

5. Develop and maintain a ransomware strategy and specific procedures that provide a formal, focused, and coordinated approach to responding to ransomware attacks.

Management Response

CFPB management concurs with our recommendation and notes that the agency is updating its incident response plans and standard operating procedure document to reflect the CFPB's ransomware response strategies. In addition, management states that the CFPB recently completed an incident response exercise that included the simulation of a ransomware incident. Lessons learned from this exercise are

¹⁰ Verizon, *2023 Data Breach Investigations Report*, March 6, 2023.

¹¹ Federal Bureau of Investigation, Internet Crime Complaint Center, *Internet Crime Report 2023*, April 4, 2024.

¹² Cybersecurity and Infrastructure Security Agency, *#StopRansomware Guide*, October 2023.

being incorporated into the agency's procedures. The CFPB expects to complete the update to the applicable plans and procedures by the fourth quarter of fiscal year 2026.

OIG Comment

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



Finding 5: Comprehensive COOP Testing Can Help Improve Organizational Resiliency

A *COOP* addresses how an organization will perform mission-essential functions in the event of an emergency, such as a natural disaster or cyberattack, for up to 30 days before returning to normal operations. Standard elements of a COOP include program plans and procedures, order of succession, risk management, and continuity of communications. According to the Federal Emergency Management Agency's continuity guidance circular, evaluation activities assess and validate continuity plans, policies, procedures, and systems using tests and exercises.¹³ COOP testing ensures that resources and procedures are kept in a constant state of readiness by evaluating the correct operation of all equipment, procedures, processes, and systems that support an organization's continuity program. Exercises provide a low-risk environment to test capabilities, familiarize personnel with roles and responsibilities, and foster meaningful interaction and communication across organizations.

The CFPB updated its COOP in 2024, identifying three mission-essential functions.¹⁴ These functions relate to the agency's mission of regulating the offering and provision of consumer financial products or services under federal consumer laws, enforcing federal consumer financial law fairly and consistently, and educating and empowering consumers in making financial decisions. Two of the three mission-essential functions were not previously designated as such. We found that while the CFPB performed COOP testing for one of its mission-essential function, it has not performed COOP testing for these two new mission-essential functions and their associated essential supporting activities.¹⁵ A CFPB official notified us that the agency did not conduct this level of testing because it prioritized updating its COOP and BIA.

Homeland Security Presidential Directive 20, National Security Presidential Directive 51, National Continuity Policy, Federal Continuity Directive, and Federal Executive Branch National Continuity Program and Requirements mandate a COOP for all organizations. Specifically, *Federal Continuity Directive* requires annual testing of alert and notification procedures for continuity personnel; primary and backup infrastructure systems and services, such as power, water, and fuel, at alternate locations; and telework capabilities. NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, also notes the importance of testing contingency plans that involve coordination, including COOP. We believe that ensuring a comprehensive test and exercise of the CFPB's COOP can help ensure organizational resilience.

¹³ Federal Emergency Management Agency, Office of National Continuity Programs, *Continuity Guidance Circular*, February 2018 (2024 update).

¹⁴ A mission-essential function is directly related to the organization's mission as set forth in its statutory or executive charter.

¹⁵ Essential supporting activities are critical processes that support mission-essential function operations during a disruption.

Recommendation

We recommend that the CAO

6. Ensure that testing of mission-essential functions identified in the CFPB's COOP is periodically performed.

Management Response

CFPB management concurs with our recommendation and notes that the previously approved mission-essential function was tested in June 2024 with the objective of troubleshooting and conducting recovery and service reconstitution activities. Further, two new mission-essential functions were identified as part of the COOP update in June 2024, and function owners are working to map and document the requirements necessary to support them in a continuity situation. In addition, management notes that testing and exercising for these two new functions is planned for the fourth quarter of fiscal year 2025 and every 2 years thereafter, in accordance with the new federal continuity directive issued in 2024.

OIG Comment

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



Finding 6: Ensuring Accurate Risk Information in the Cybersecurity GRC Tool Can Help Prioritize Risk Responses

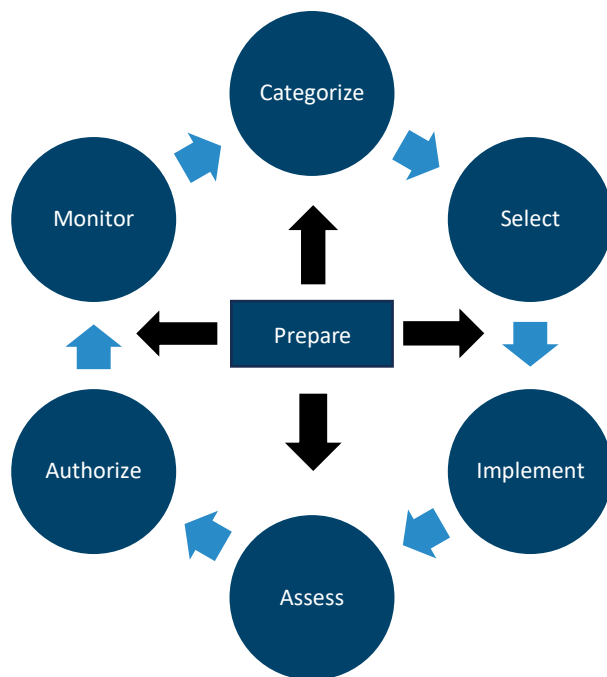
The CFPB uses a GRC tool to gain a centralized view of cybersecurity risks across the agency. This tool is provided as a shared service from another federal agency, and it enables the CFPB to automate its FISMA inventory tracking, monitor ongoing authorization processes, and manage its system-level plans of action and milestones. We found that the CFPB's GRC tool contained inaccurate information on system categorization levels for 68 of 236 agency systems. Specifically, the system categorization level in the GRC tool for these 68 systems did not reflect the high-watermark risk levels assigned to the confidentiality, integrity, and availability of security objectives. In addition, the GRC tool had inaccurate expiration dates for the authorizations to operate (ATOs)¹⁶ or authorizations to use (ATUs)¹⁷ for 14 systems.

NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, presents a seven-step process that organizations can use to manage security and privacy risks to their information systems (figure 1).

¹⁶ An ATO is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the nation based on the implementation of an agreed set of security and privacy controls.

¹⁷ An ATU is employed when an organization chooses to accept the information in the ATO granted by another organization, such as is the case for the CFPB's GRC tool. The ATU is a mechanism to promote reciprocity for systems under the purview of different authorizing officials. The official issuing an ATU has the same level of responsibility and authority for risk management as an authorizing official issuing an ATO.

Figure 1. NIST's Risk Management Framework for Information Systems



Source: OIG representation of information in National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, December 2018.

The purpose of the *categorize* step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, and the nation, with respect to the security loss of confidentiality, integrity, and availability of the system. NIST Special Publication 800-37 further states that as part of system categorization, the impact levels (*high*, *moderate*, *low*) are to be determined for each information type and for each security objective; the security categorization of the system is based on a high watermark of information-type impact levels. In addition, the purpose of the *authorize* step is to provide organizational accountability by requiring a senior management official to determine whether the security and privacy risks faced by the system have been reduced to an acceptable level.

We attribute these inaccuracies in the CFPB's GRC tool to three factors. First, system owners were not ensuring that accurate information was entered in the tool. Second, the CFPB did not consistently review the information entered in the GRC tool to ensure accuracy. Third, the CFPB had not renewed an ATU for its GRC tool, which would have included an assessment of the tool's input validation controls to ensure that data inputs are accurate and correct.

While the categorization ratings for the 68 systems were inaccurate in the CFPB's GRC tool, we did not identify an impact to the security control baselines applied for the systems. The security control baselines were not affected because the CFPB maintains accurate categorization ratings outside the GRC tool. Further, for the 14 systems that had inaccurate expiration dates for their ATOs and ATUs, none was operating with expired ATOs or ATUs. However, we believe that accurate information in the GRC tool will

assist the CFPB with efforts to automate risk management activities and ensure that resources are prioritized to address the most critical security vulnerabilities.

Recommendations

We recommend that the CIO

7. Renew the ATU for the CFPB's GRC tool.
8. Implement a process that ensures the cyber risk information in the CFPB's GRC tool is accurate and maintained.

Management Response

CFPB management concurs with our recommendations. In response to recommendation 7, CFPB management states that the agency leverages federal shared services to support the GRC and issues an ATU for this service annually. Management notes that the agency plans to complete the ATU by the first quarter of fiscal year 2025 and annually thereafter.

In response to recommendation 8, CFPB management states that the agency will continue to update the GRC tool and processes to ensure data quality improvements related to system categorization levels. The CFPB expects to have these updates completed by the second quarter of fiscal year 2025.

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.



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 five function areas outlined in the *FY 2023–2024 IG FISMA Reporting Metrics*. These five function areas are *identify, protect, detect, respond, and recover*. The five function areas consist of nine security domains: risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

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

- used a risk-based approach and focused our detailed testing activities on the annual core metrics and supplemental FY 2024 metrics identified in the *FY 2023–2024 IG FISMA Reporting Metrics*
- 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 level¹⁸
- performed data analytics using commercially available tools to support our testing in multiple security domains

To determine whether the CFPB's information security program is effective, we used the scoring methodology defined in the *FY 2023–2024 IG FISMA Reporting Metrics*. In accordance with the 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 conclusion. Our specific maturity ratings at the function and domain levels were entered in the CyberScope FISMA reporting application.

We conducted this work from February 2024 to July 2024. 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.

¹⁸ We selected systems using a risk-based approach that includes factors such as the system's purpose, the information maintained within the system, and the function of the system. Our testing of these selected systems did not result in any new program-level findings that are presented in this report.



Appendix B: Status of Prior FISMA Recommendations

As part of our 2024 FISMA audit, we reviewed the actions taken by the CFPB to address the outstanding recommendations from our prior FISMA audit reports. Below is a summary of the status of the seven recommendations that were open at the start of our 2024 FISMA audit (table B-1). We are closing four recommendations, which are related to software asset management, configuration management, and contingency planning. We will update the status of these recommendations in our fall 2024 semiannual report to Congress, and we will continue to monitor the CFPB's progress in addressing our open recommendations as a part of our future FISMA audits.

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

Year	Recommendation	Status	Explanation
Risk management			
2022	3	Closed	We recommend that the CIO ensure that policies and supporting procedures for developing and maintaining an enterprisewide software inventory are developed and maintained. The CFPB has developed policies and supporting procedures for maintaining an enterprisewide software inventory.
2022	4	Open	We recommend that the CIO ensure that an enterprisewide software inventory is conducted and maintained. The CFPB is in the process of conducting an enterprisewide software inventory.
Configuration management			
2018	1	Closed	We recommend that the CIO strengthen configuration management processes by (a) remediating configuration-related vulnerabilities in a timely manner and (b) ensuring that optimal resources are allocated to perform vulnerability remediation activities. We are closing this recommendation and issuing a new recommendation in this report that is more specifically targeted at root causes for the configuration management vulnerabilities we continue to find.

Year		Recommendation	Status	Explanation
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	The CFPB plans to implement a new automated tool to manage its user-access agreements and rules-of-behavior forms for privileged users. After the end of our fieldwork, CFPB officials provided additional information and requested closure of this recommendation. We plan to follow up as part of future audits.
Contingency planning				
2022	5	We recommend that the CIO, in coordination with the CAO, ensure the development of policies and procedures for the performance and maintenance of an organizationwide BIA.	Closed	The CFPB developed policies and procedures to support the performance and maintenance of an organizationwide BIA.
2022	6	We recommend that the CIO, in coordination with the CAO, update the CFPB's organizationwide BIA and ensure that the results are used to make applicable changes to related contingency and continuity plans.	Closed	The CFPB has updated its organizationwide BIA and ensured that the results are used to make applicable changes to related contingency and continuity plans.
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 expects to complete the development of policies and supporting procedures, as well as the contingency plan testing schedule, by the fourth quarter of FY 2025.

Source: OIG analysis.

Appendix C: Management Response



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

October 29, 2024

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 *2024 Audit of the CFPB's Information Security Program*. We are pleased that you found the Consumer Financial Protection Bureau's (CFPB) Information Security Program continues to operate effectively at a level 4 (*managed and measurable*) maturity based on the Federal Information Security Modernization Act of 2014 (FISMA) maturity model. In Fiscal Year (FY) 2025, the CFPB will continue to enhance its processes and technologies to strive for the level 5 (*Optimized*) maturity rating and address cited recommendations.

We understand the FISMA audit evaluation methodology consists of an annual assessment of core metrics and a biennial assessment of select supplemental metrics. The metrics are grouped into nine security domains, which align with the five functions in the Cybersecurity Framework (*identify, protect, detect, respond, recover*) to determine the overall maturity of the CFPB's information security program. Furthermore, the draft report states the following and the CFPB offers responses to these statements:

- **Identify:** The CFPB continues to operate at level-3 maturity (*consistently implemented*). The CFPB has implemented processes in the areas of risk management and supply chain risk management and uses a Governance Risk and Compliance (GRC) tool to gain a centralized view of cybersecurity risks across the agency. In FY2025, the CFPB will make

consumerfinance.gov

improvements to the accuracy of information in the CFPB's GRC tool to assist the CFPB with efforts to automate risk management activities and ensure that resources are prioritized to address the most critical security vulnerabilities.

- **Protect:** The CFPB continues to operate at level-3 maturity (*consistently implemented*). The CFPB has strengthened its security training program by incorporating threat intelligence to update its workforce on a near-real-time basis, resulting in the agency's first level-5 (*optimized*) maturity rating for a FISMA metric. Additionally, the CFPB has strengthened its data loss prevention (DLP) function. In FY2025, the CFPB will take several actions to improve this function: 1) The CFPB will finalize an agencywide data classification policy and use those classifications to improve DLP and to better protect CFPB data; 2) The CFPB will make efforts to ensure that users' continued access to systems is contingent upon a favorable reinvestigation, to better protect the CFPB against insider threats; 3) The CFPB will seek to improve our configuration management database to include additional aspects to support timely mitigation of technical vulnerabilities to reduce the attack surface's risk to known threats.
- **Detect:** The CFPB continues to operate effectively at level-4 maturity (*managed and measurable*) for the Detect function. The CFPB has implemented effective information security continuous monitoring (ISCM) program and continues to improve its automation capabilities with the goal of eventually incorporating advanced technologies to continuously improve its ISCM capabilities on a near real-time basis. In FY2025, the CFPB will strive for a level 5 (*optimized*) maturity in this area.
- **Respond:** The CFPB continues to operate at level-4 maturity (*managed and measurable*). The CFPB has developed strategies, policies, and procedures to respond to various cybersecurity incidents and implemented technologies to assist the incident response team in effectively responding to incidents. In FY2025, the CFPB will incorporate strategies that focus on ransomware attacks into CFPB's incident response plans and procedures to prepare for the rising prevalence of ransomware attacks and recover in the case a ransomware incident.
- **Recover:** The CFPB's maturity increased from a level-2 (*defined*) maturity to a level 3 (*consistently implemented*). The CFPB updated its enterprise business impact analysis (BIA) and ensured that the results are used to make applicable changes to related contingency and continuity plans. In FY2025, the CFPB will test the new mission essential functions and their associated essential supporting activities identified in the updated continuity of operations plan (COOP).

We acknowledge that we can mature our information security program in the areas of data loss prevention, vulnerability remediation, personnel security, incident management, contingency planning, and risk management. We appreciate the OIG for noting CFPB's progress on remediating recommendations from previous OIG audits. We value your objective and independent viewpoints and consider our OIG to be a trusted source of informed, accurate, and insightful information.

Thank you for the professionalism and courtesy that you and all the OIG personnel showed throughout this review. Our response to the cited recommendation is below.

Sincerely,

CHRISTOPHE
R CHILBERT

Digitally signed by
CHRISTOPHER CHILBERT
Date: 2024.10.29 12:49:14
-04'00'

Christopher Chilbert
Chief Information Officer

Response to recommendations presented in the OIG Draft Report: 2024 Audit of the CFPB's Information Security Program

Recommendation 1: Complete finalization of an agencywide data classification policy that accounts for the sensitivity of the data maintained by the CFPB.

Management Response:

The CFPB concurs with this recommendation. The CFPB has taken steps to develop and implement a Controlled Unclassified Information (CUI) program, including drafting a CUI policy that outlines roles and responsibilities and identifies thirteen (13) categories of CUI. The Chief Data Officer, who will serve as the Senior Agency Official, has appointed the Senior Records Management Specialist as the CUI Program Manager. We expect to complete the CUI policy by FY2025 Q4.

Recommendation 2: Ensure that data classification and sensitivity labels are incorporated into the CFPB's DLP program.

Management Response:

The CFPB concurs with this recommendation. The CFPB has already aligned the data loss prevention trigger rules with the draft CUI policy and is prepared to make any remaining changes as soon as the CUI policy is finalized. We expect to complete these updates by FY2026 Q1.

Recommendation 3: 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.

Management Response:

The CFPB concurs with this recommendation. The T&I Enterprise Architecture & Governance team's ongoing "improved configuration management database (CMDB) project" will address a portion of this recommendation by integrating additional data sources into the CMDB, which will provide mapping of remediation owners to system IP addresses and host names. The Cybersecurity and Enterprise Platform teams will work together to develop and implement a process to ensure accuracy in the CMDB mapping. Additionally, the CFPB has initiated an automated process and program to identify operating system and application vulnerabilities, established a regular cadence to review these with system owners, and provides regular reporting

to T&I leadership on remediation progress. The refinements to the program described in the recommendations will further enhance accountability and highlight resource constraints to prioritize risk management efforts. We expect to complete these updates by FY2026 Q4.

Recommendation 4: Ensure that adequate resources are allocated to re-investigate CFPB systems users as required.

Management Response:

The CFPB concurs with this recommendation. The CFPB's Personnel Security policy requires individuals to undergo a re-investigation every 5 years and the Personnel Security team prioritizes the oldest cases for reinvestigation. Due to a number of competing priorities such as the influx of new employee onboarding, integration work between the background investigation systems, and addressing multiple policy matters, the re-investigations have been delayed approximately one year. Additionally, the nature of the background investigation process and reliance on other agencies (e.g., Defense Counterintelligence and Security Agency (DCSA), Office of Personnel Management (OPM)), increase the potential for delays in this process and a common occurrence across the government. To successfully complete the re-investigations, the CFPB is exploring options to clear the backlog, such as considering greater resource allocation in the form of personnel and/or funding to the DCSA. We have prioritized the completion of the backlog of re-investigations and expect completion by FY2026 Q4.

Recommendation 5: Develop and maintain a ransomware strategy and specific procedures that provide a formal, focused, and coordinated approach to responding to ransomware attacks.

Management Response:

The CFPB concurs with this recommendation. The CFPB's Cybersecurity Incident Response Team (CSIRT) is updating the content of the Standard Operating Procedure (SOP) and Cybersecurity Incident Response and Recovery Plan (IRRP) to reflect the CFPB's ransomware response strategies. In addition, CFPB recently completed our annual Cybersecurity Incident Response exercise, which featured scenarios simulating ransomware incident impacting multiple CFPB business and system functions; CFPB is incorporating those lessons learned in our procedures as well. We expect to complete the update to the applicable plans and procedures by FY2026 Q4.

Recommendation 6: Ensure that testing of mission essential functions identified in the CFPB's COOP is periodically performed.

Management Response:

The CFPB concurs with this recommendation. In accordance with the new Federal Continuity Directive issued in 2024, agencies are only required to conduct an exercise for each mission essential function (MEF) biennially to validate its ability to sustain performance of the essential function. The previously approved MEF under Consumer Response was tested in June 2024 with the objective of troubleshooting and conducting recovery and service reconstitution activities. The updated COOP plan was signed in June 2024, and it included the identification of two (2) new MEFs. The new MEF owners have been diligently working to map and document the requirements necessary to support the MEFs in a continuity situation. While it was not feasible to conduct a test of the newly identified MEFs in FY2024, that testing/exercising is planned for FY2025 Q4 and every 2 years thereafter.

Recommendation 7: Renew the ATU for the CFPB's GRC tool.

Management Response:

The CFPB concurs with this recommendation. The CFPB leverages a federal shared services to support governance, risk, and compliance (GRC) and issues an authorization to use this service annually. The CFPB is expected to complete re-authorization of the CFPB's GRC tool by FY2025 Q1 and annually thereafter.

Recommendation 8: Implement a process that ensures the cyber risk information in the CFPB's GRC tool is accurate and maintained.

Management Response:

The CFPB concurs with this recommendation. Due to the CFPB's GRC tool's mandatory update, the CFPB system categorizations defaulted to low-watermark risk level for all new systems. The CFPB will continue to update the GRC tool and processes to ensure data quality improvements to reflect high-watermark risk levels in alignment with the system owner's signed system categorization documentation. We expect to have these updates completed by FY2025 Q2.



Abbreviations

ATO	authorization to operate
ATU	authorization to use
BIA	business impact analysis
CAO	chief administrative officer
CIO	chief information officer
COOP	continuity of operations plan
CUI	controlled unclassified information
Cybersecurity Framework	<i>Framework for Improving Critical Infrastructure Cybersecurity</i>
DLP	data loss prevention
FISMA	Federal Information Security Modernization Act of 2014
GRC	governance, risk, and compliance
IG	inspector general
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

Report Contributors

Paul Vaclavik, Senior OIG Manager for Information Technology Audits

Chelsea Nguyen, OIG Manager, Information Technology Audits

Nilesh Patel, Senior IT Auditor

Deyanara Gonzalez, IT Auditor

Justin Byun, IT Auditor

Christy Alcaraz, IT Auditor

Andrew Luckman, Forensic Auditor

Khalid Hasan, Assistant Inspector General for Information Technology

Contact Information

General

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

Phone: 202-973-5000

Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov



Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

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

Phone: 800-827-3340

Fax: 202-973-5044