Audit Report
2023-IT-C-016
September 29, 2023

Consumer Financial Protection Bureau

2023 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

MEMORANDUM

DATE: September 29, 2023

TO: Chris Chilbert
Chief Information Officer
Consumer Financial Protection Bureau

FROM: Khalid Hasan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2023-IT-C-016: *2023 Audit of the CFPB's Information Security Program*

This memorandum transmits the subject audit report, prepared by Cotton & Company Assurance and Advisory, LLC. We contracted with Cotton to conduct a performance audit of the Consumer Financial Protection Bureau's information security program.

The contract requires the audit to be performed in accordance with generally accepted government auditing standards. We reviewed and monitored the work of Cotton to ensure compliance with the contract. Cotton is responsible for the accompanying report, *2023 Audit of the CFPB's Information Security Program*, dated September 29, 2023.

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

cc: Jan Singelmann
Adam Martinez
Jean Chang
Tiina Rodrigue
Kathryn Fong
Ren Essene
Jafnar Gueye
Martin Michalosky
Marianne Roth
Richard Austin
Tacy Summersett
Ashley Adair
Brandi Mix Womack

2023 AUDIT OF THE CFPB'S INFORMATION SECURITY PROGRAM

SUBMITTED TO THE OFFICE OF INSPECTOR GENERAL OF THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM AND THE CONSUMER FINANCIAL PROTECTION BUREAU

FINAL AUDIT REPORT

SEPTEMBER 29, 2023

Cotton
A SIKICH COMPANY

COTTON, A SIKICH COMPANY
333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701
Harrison.Lee@sikich.com | www.cottoncpa.com

Cotton
A SIKICH. COMPANY

333 John Carlyle Street, Suite 500 | Alexandria, VA 22314
P: 703.836.6701 | www.cottoncpa.com

September 29, 2023

To: Inspector General, Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau

Subject: 2023 Audit of the CFPB's Information Security Program

Cotton & Company Assurance and Advisory, LLC (Cotton), is pleased to provide the Office of Inspector General (OIG) for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau (CFPB) with our independent performance audit report of the CFPB's information security program. We performed this audit pursuant to requirements in the Federal Information Security Modernization Act of 2014 (FISMA). Specifically, FISMA requires each agency inspector general (IG) to conduct an annual independent evaluation of the effectiveness of their agency's information security program and practices. To meet these requirements, the OIG contracted Cotton to assess the effectiveness of the CFPB's information security program across the core and supplemental metrics outlined in the Office of Management and Budget's (OMB's) *Fiscal Year 2023-2024 IG FISMA Reporting Metrics*. We also reviewed security controls for select agency systems. We performed the work from March through August 2023.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, as amended, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Sincerely,
Cotton & Company Assurance and Advisory, LLC

Harrison Lee, CISA, CISM, CISSP, PMP
Partner, Cotton

EXECUTIVE SUMMARY

Report on the 2023 Audit of the Consumer Financial Protection Bureau's Information Security Program

Findings

The Consumer Financial Protection Bureau's (CFPB's) information security program continues to operate effectively at Maturity Level 4: Managed and Measurable. We found that, since fiscal year (FY) 2022, the CFPB has taken steps to broadly strengthen its information security program. In particular, we found that the CFPB has improved the maturity of its information security continuous monitoring and supply chain risk management processes and made improvements in its efforts to meet the zero-trust architecture requirements.

We identified opportunities to strengthen the CFPB's information security program in the areas of asset management and data loss protection. In addition, we found that the CFPB can maintain resilience by ensuring that it schedules and performs contingency plan testing at least annually for all its systems. We also found that the CFPB can improve its continuity of operations processes by ensuring that it conducts and maintains an organization-wide business impact analysis.

Finally, we found that the CFPB has taken sufficient actions to close four recommendations that the OIG reported on in its prior Federal Information Security Modernization Act of 2014 (FISMA) audit reports and that remained open at the start of this audit. These recommendations related to the CFPB's account management, risk management, configuration management, and identity and access management processes. The Office of Inspector General of the Board of Governors of the Federal Reserve System will update the status of these recommendations in its Fall 2023 semiannual report to Congress and will continue to monitor the CFPB's progress as part of future FISMA audits.

Recommendations

This report includes one new recommendation designed to strengthen the CFPB's information security program with regard to contingency planning.

Purpose

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

Background

FISMA requires each agency inspector general (IG) to conduct an annual independent evaluation of their agency's information security program, practices, and controls for select systems. The Office of Management and Budget's (OMB's) *Fiscal Year 2023-2024 IG FISMA Reporting Metrics* directs IGs to evaluate the maturity level of their agency's information security program for FY 2023, from a low of 1 to a high of 5. OMB notes that Level 4: Managed and Measurable represents an effective level of security.

REPORT ON THE 2023 AUDIT OF THE CFPB'S INFORMATION SECURITY PROGRAM

Finding 1: The CFPB Can Improve Its Software Asset Management Processes by Implementing a Standard Taxonomy

Number	Recommendation	Responsible Office
N/A	We are not making a new recommendation for this finding because it is related to open recommendations from OIG's 2022 Audit of the CFPB's Information Security Program. More details are available in Appendix B.	Office of Technology and Innovation

Finding 2: The CFPB Can Strengthen Its Data Loss Prevention Capabilities

Number	Recommendation	Responsible Office
N/A	We are not making a new recommendation for this finding because it is related to open recommendations from OIG's 2022 Audit of the CFPB's Information Security Program. More details are available in Appendix B.	Office of Technology and Innovation

Finding 3: The CFPB Can Improve Its Resilience by Testing Its Contingency Plans

Number	Recommendation	Responsible Office
1	Maintain a comprehensive schedule for testing current contingency plans, documenting test procedures, and maintaining relevant updates to the contingency plan.	Office of Technology and Innovation

Finding 4: The CFPB Can Update Its Organization-wide Business Impact Analysis

Number	Recommendation	Responsible Office
N/A	We are not making a new recommendation for this finding because it is related to open recommendations from OIG's 2022 Audit of the CFPB's Information Security Program. More details are available in Appendix B.	Office of Technology and Innovation and the Office of Administrative Operations

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Objectives

In support of the Federal Information Security Modernization Act of 2014 (FISMA),[1] the Office of Inspector General (OIG) for the Board of Governors of the Federal Reserve System contracted Cotton & Company Assurance and Advisory, LLC (Cotton), to conduct an audit to assess the effectiveness of the Consumer Financial Protection Bureau's (CFPB's) information security program. The audit objectives, based on the 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. Please see Appendix A for additional information regarding our scope and methodology.

1.2 Background

FISMA requires agencies to develop, document, and implement an agency-wide security program for the information and information systems that support the agency's operations and assets, including information and information systems provided by another agency, a contractor, or another source. FISMA also requires that each agency's inspector general (IG) perform an annual independent evaluation to determine the effectiveness of the agency's information security program and practices, including testing the effectiveness of information security policies, procedures, and practices for select systems. To support these independent evaluation requirements, the Office of Management and Budget (OMB), the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders worked collaboratively to develop the *Fiscal Year (FY) 2023-2024 IG FISMA Reporting Metrics*. The *FY 2023-2024 IG FISMA Reporting Metrics* represent a continuation of the work started in FY 2022, when the reporting process for the IG FISMA metrics transitioned to a multi-year cycle (see Figure 1).[2]

Figure 1. Multi-Year IG FISMA Reporting Cycle

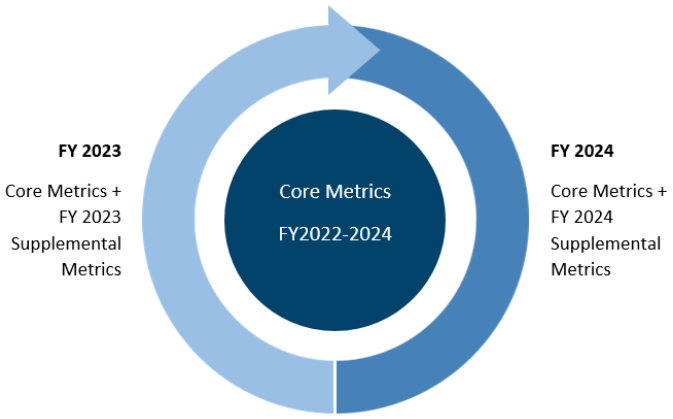

Figure 1 Source: Cotton analysis of OMB Memorandum M-22-03, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements

As part of this transition, OMB implemented a new framework for the timing and focus of annual IG FISMA assessments, with the goal of providing a more flexible and continued focus on annual assessments for the federal community. This effort yielded two distinct groups of metrics for IGs to assess in their annual FISMA reviews: core metrics and supplemental metrics.

[1] Federal Information Security Modernization Act of 2014, Public Law (Pub. L.) No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S. Code §§ 3551–3558).
[2] OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, December 2, 2022.

- **Core metrics** are metrics that IGs must assess annually. Core metrics represent a combination of administration priorities, high-impact security processes, and essential functions that are necessary to determine the effectiveness of an agency's security program.
- **Supplemental metrics** are metrics that IGs must assess at least once every 2 years. Supplemental metrics represent important activities conducted by security programs. They contribute to the overall evaluation and determination of the security program's effectiveness.

The IG FISMA metrics (both core and supplemental) are grouped into nine security domains, which align with the five function areas in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover (see Table 1).[3] The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance in assessing the maturity of controls to address those risks.

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

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

Table 1 Source: U.S. Department of Homeland Security, FY 2021 IG FISMA Reporting Metrics

1.2.1 FISMA Maturity Model

OMB's *FY 2023–2024 IG FISMA Reporting Metrics* states that IGs are required to assess the effectiveness of their agency's information security program by assessing the core and supplemental metrics against a maturity model spectrum.[4] The five levels of the maturity model are:

1. Ad Hoc
2. Defined

[3] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.
[4] As noted in the *FY 2023-2024 IG FISMA Reporting Metrics*, IGs should use the CyberScope application to submit the results of their core metrics evaluation. As such, the OIG used the CyberScope application to provide the Department of Homeland Security (DHS) with detailed responses and assessment of the CFPB's progress in

3. Consistently Implemented
4. Managed and Measurable
5. Optimized

The foundational levels of the model (1–3) are geared toward the development and implementation of policies and procedures, while the advanced levels (4–5) capture the extent to which agencies institutionalize those policies and procedures (see Figure 2). As noted in the *FY 2023–2024 IG FISMA Reporting Metrics*, OMB believes that, within the context of the maturity model, achieving at least Level 4: Managed and Measurable represents an effective level of security.[5] Appendix A includes further details regarding the scoring methodology for the maturity model.

Figure 2. FISMA Maturity Model Rating Scale

Figure 2 Source: Cotton analysis of OMB's FY 2023–2024 IG FISMA Reporting Metrics, February 10, 2023.

implementing the core metrics. Given the sensitive nature of these responses, they are restricted and are not included in this report.

[5] NIST defines security and privacy control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the designated security and privacy requirements. (NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, updated December 10, 2020.)

2 SUMMARY OF THE CFPB'S INFORMATION SECURITY PROGRAM

We found that overall, the CFPB's information security program continues to operate effectively at maturity model Level 4: Managed and Measurable. Since FY 2022, the CFPB has continued to strengthen its information security program. The CFPB continues to add automation to its information security continuous monitoring (ISCM) processes that will provide additional insights regarding risk management and incident response. For example, the CFPB's supply chain risk management processes incorporate vendor risk information for improved risk-based decision-making. In addition, the CFPB continues to strengthen its zero-trust architecture (ZTA) by incorporating strong authentication processes into its application management, including cloud-based services.

As in the prior year, we identified opportunities for the CFPB to mature its information security program in the areas of data loss prevention (DLP), software asset management, and continuity planning to ensure that its program remains effective. The similarity between the FY 2022 and FY 2023 findings occurred because unforeseen project and procurement delays negatively impacted the CFPB's project milestones. The table below compares the overall ratings in FY 2023 with FY 2022 and 2021 for each of the NIST Cybersecurity Framework functions. This year, there was general improvement for most of the FISMA metrics, which contributed to improved scoring for the Identify and Protect functions. The decrease in the Recover function can be attributed, in part, to the change from mode scoring to average scoring.[6]

Figure 3: Maturity of the CFPB's Information Security Program by Security Function, 2021 to 2023

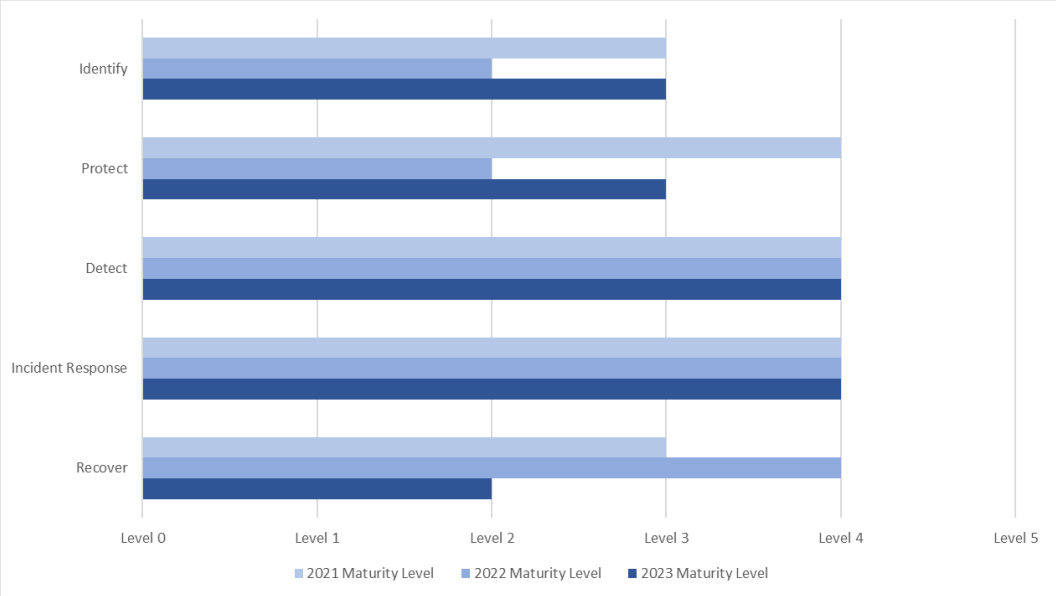

Figure 3 Source: Auditor Analysis

[6] Per the *FY 2023-2024 IG FISMA Reporting Metrics*, pages 8-10, the scoring methodology for FY 2023 was changed. Specifically, scoring is based on the calculated average score of the metrics in a particular domain with a focus on the results of the core metrics.

2.1 Analysis of the CFPB's Progress in Implementing FISMA Information Security Program Requirements

2.1.1 Identify Function Summary

Figure 4: Identify Function—Level 3: Consistently Implemented

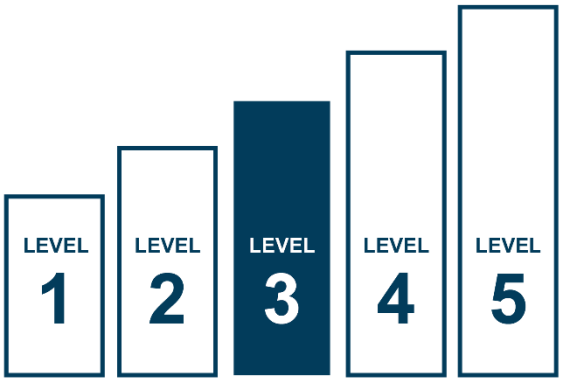

Figure 4 Source: Auditor Analysis

The CFPB's Identify function is operating at Maturity Level 3: Consistently Implemented. The CFPB has demonstrated improvements regarding the Identify function's risk management domain in areas such as asset management for both hardware and software. These include demonstrated improvements in processes and procedures. In addition, the CFPB is integrating risk management tools into numerous other domains, such as configuration management, information system continuous monitoring, and incident response. These tools include, but are not limited to, areas such as automated control assessments, asset discovery, and continued implementation of the change management database (CMDB). The CFPB has also demonstrated significant improvement in its management of Plans of Action and Milestones (POA&Ms).

The CFPB also demonstrated improvements in its supply chain risk management processes, including improved procurement processes that incorporate risk management activities. The CFPB has also incorporated processes for using third-party vendor information in both pre- and post-procurement activities.

We identified areas for improvement in software inventory management and noted that there are three open recommendations in this area from previous FISMA reports. These recommendations relate to risk appetite and tolerance, as well as software inventories. See Appendix B for additional information regarding these recommendations.

Findings

The CFPB Can Improve Its Software Asset Management Processes by Implementing a Standard Taxonomy

The CFPB demonstrated that it is gathering information about software assets from various resources, such as asset discovery; however, it was unable to provide a uniform list of software assets that would allow for organizational inventory management and reconciliation. NIST Special Publication (SP) 800-53, Revision 5, control CM-8, System Component Inventory, states, in part, that the organization must:

> *Develop and document an inventory of system components that:*
>
> *a) Accurately reflects the system;*

b) Includes all components within the system;
c) Is at the level of granularity deemed necessary for tracking and reporting; and
d) *Includes the information to achieve system component accountability*

The OIG's FY 2022 FISMA report made recommendations for improvements in policies and procedures related to software asset management and conducting an enterprise-wide software inventory.[7] We also found that the CFPB does not maintain a uniform list of software assets, and the lists that the CFPB did provide contained different asset information. The CFPB lacks a formal software asset management unified taxonomy that defines elements at the level of granularity required for managing those assets. A software taxonomy plays a crucial role in categorizing and classifying software applications based on various criteria, such as their purpose, functionality, criticality, and licensing terms. Without this structure in place, there is a higher risk of inconsistencies, redundancies, and difficulties in tracking and understanding the CFPB's software management, as well as an increased chance of unauthorized software existing on CFPB systems.

Recommendation
We are not making a new recommendation for this finding because it is related to open recommendations 2022-IT-C-014.3 and 2022-IT-C-014.4 from the OIG's 2022 Audit of the CFPB's Information Security Program. Additional information is available in Appendix B.

We have included this finding for management consideration.

[7] OIG, *2022 Audit of the CFPB's Information Security Program,* OIG Report 2022-IT-C-014, September 30, 2023.

2.1.2 Protect Function Summary

The CFPB's Protect function is operating at Maturity Level 3: Consistently Implemented. The CFPB creates and maintains baseline configurations based on security assessments and uses these configurations for tracking and reporting. In addition, the CFPB has made progress in integrating with DHS's Continuous Diagnosis and Mitigation program to improve its ability to monitor and manage network operations. Further, the CFPB is more effectively managing stakeholders for areas under the Identify and Access Management functions, which should encourage continued improvements in account management. In addition, the CFPB has continued to expand its use of phishing-resistant authentication, such as multi-factor authentication (MFA), further strengthening its authentication mechanisms.

Figure 5: Protect Function—Level 3: Consistently Implemented

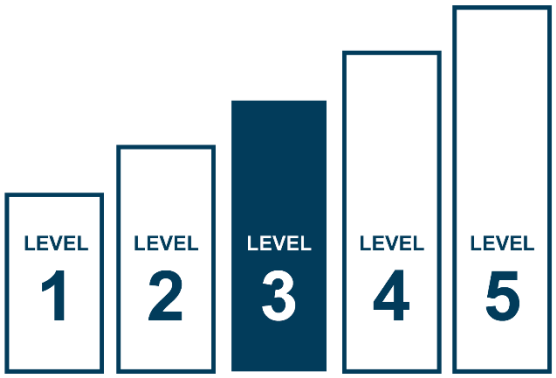

Figure 5 Source: Auditor Analysis

The CFPB has defined its data privacy processes and has implemented processes such as privacy assessments to manage personally identifiable information (PII) and other sensitive information. The CFPB also continues to maintain a security training program for both general users and privileged users. The CFPB was able to demonstrate that it provides training to meet organizational needs while also providing adaptive resources to meet user needs.

We did note that the CFPB could improve its protection of sensitive data by implementing an organization-wide DLP solution. In addition, there are four open recommendations from previous FISMA reports related to configuration management, account management, and data loss protection. Additional information regarding these recommendations is available in Appendix B.

Findings

The CFPB Can Strengthen Its Data Loss Prevention Capabilities

OMB Memorandum M-22-09 requires federal agencies to implement ZTA. ZTA requires organizations to assume that a breach has already occurred or is currently occurring. As part of a ZTA solution, organizations should perform all communication in the most secure manner available, protect confidentiality and integrity, and provide source authentication. DLP solutions meet the ZTA requirement, as they serve as automated tools to monitor PII both internally and at network boundaries for unusual or suspicious transfers or events. In addition, NIST SP 800-53, Revision 5, control SI-4, System Monitoring, states, in part:

> *(4) System Monitoring | Inbound And Outbound Communications Traffic*
>
> > *(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;*
> >
> > *(b) Monitor inbound and outbound communications traffic*

(18) System Monitoring | Analyze Traffic And Covert Exfiltration

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information

NIST SP 800-53, Revision 5, SI-7, Boundary Protection, states, in part:

(10) Boundary Protection | Prevent Exfiltration

(a) Prevent the exfiltration of information; and

(b) Conduct exfiltration tests[8]

The FY 2022 FISMA report made recommendations for creating policies and procedures related to implementing a DLP tool.[9] The CFPB has partially implemented these recommendations by deploying tools to increase DLP functions in its architecture. However, the CFPB has not yet implemented a network-based organizational DLP system because it has encountered delays in deploying a new DLP platform.

Recommendation
We are not making a new recommendation for this finding because it is related to open recommendation 2022-IT-C-014.2 from OIG's 2022 Audit of the CFPB's Information Security Program. Additional information is available in Appendix B.

We have included this finding for management consideration.

[8] NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations,* Revision 5, updated December 10, 2020.
[9] OIG, *2022 Audit of the CFPB's Information Security Program,* OIG Report 2022-IT-C-014, September 30, 2023.

2.1.3 Detect Function Summary

The CFPB's Detect function is operating at Maturity Level 4: Managed and Measurable. The CFPB has maintained a continuous monitoring program that positively impacts its other FISMA functions, such as Identify, Protect, and Respond. The CFPB's vulnerability management program maintains strong communication with both business and information technology stakeholders to remediate issues. In addition, the CFPB maintains a continuous assessment program that supports various other programs, such as system authorizations and risk assessments. The CFPB is moving to automate tools to further improve its communication and transparency. The CFPB also continues to enhance its monitoring with various initiatives, including the DHS CDM program.

Figure 6: Detect Function—
Level 4: Managed and Measurable

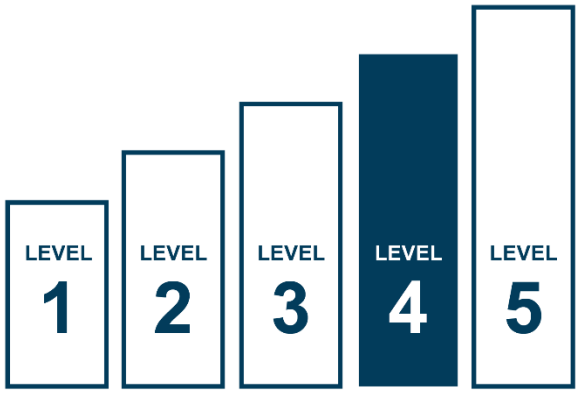

Figure 6 Source: Auditor Analysis

We found that the Detect function was operating effectively and therefore did not identify any findings related to this function. The CFPB is continuing 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 order to reach Maturity Level 5: Optimized.

2.1.4 Respond Function Summary

The CFPB's Respond function is operating at Maturity Level 4: Managed and Measurable. The CFPB maintains an incident response program that enables it to respond to incidents identified by various stakeholders, including collaborating with external organizations. The CFPB demonstrated that it has incident-handling processes in place and that it is deploying orchestrated incident response technologies. The CFPB also demonstrated the degree to which it has automated its incident response procedures, thereby strengthening its ability to allocate resources using risk-based decision-making, including considering risks such as the criticality of a threat.

Figure 7: Respond—
Level 4: Managed and Measurable

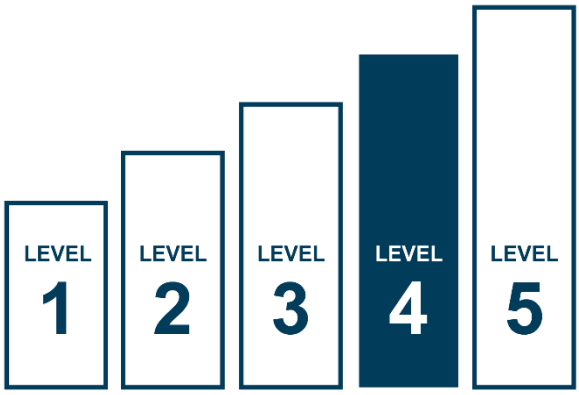

Figure 7 Source: Auditor Analysis

We found that the Respond function was operating effectively and therefore did not identify any findings related to this function. The CFPB is exercising opportunities for improvement by continuing to automate processes and improving its collaboration with external entities. The CFPB is also improving its ability to automate its use of Help Desk resources, including using automated ticket generation and improving communication with stakeholders.

2.1.5 Recover Function Summary

The CFPB's Recover function is operating at Maturity Level 2: Defined. The CFPB has developed and implemented contingency planning policies, processes, and procedures, and it has implemented contingency plan testing for the majority of the CFPB's systems. The CFPB captures feedback when testing its systems to assist in planning further testing at the system level, and it uses this feedback to update related plans, such as Information System Contingency Plans (ISCPs).

Figure 8: Recover—Level 2: Defined

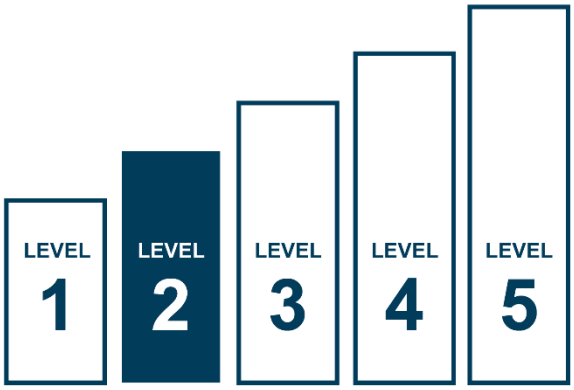

Figure 8 Source: Auditor Analysis

We found that the CFPB does have opportunities to improve its Recover function by implementing similar, consistent processes and procedures at the organizational level. The lack of contingency planning for the organization may prevent the CFPB from responding adequately to disruptive events. In addition, although the CFPB generally manages and tests ISCPs and other plans, we identified systems that the CFPB did not test in accordance with agency annual testing requirements. Specifically, the CFPB had not tested one Executive Order (EO) critical system since FY 2021, and it had scheduled testing for two other systems but had not yet completed the testing. The CFPB should ensure that it tests all ISCPs in accordance with its policy. These plans are essential for restoring critical functions and could help to mitigate a lack of planning at higher levels of the organization.

In addition, there are two open recommendations from previous FISMA reports related to contingency planning. Additional information regarding these recommendations is available in Appendix B.

Findings

The CFPB Can Schedule and Test Information Technology Contingency Plans

NIST describes contingency planning for systems as part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency plans address system restoration and implementation of alternative missions or business processes when systems are compromised or breached. Organizations must test contingency plans to determine the effects of contingency operations on organizational operations, assets, and individuals. Organizations then evaluate the results of these tests, giving the organization an opportunity to initiate corrective actions to improve the plan if needed.[10]

The CFPB demonstrated that it performed contingency plan testing for various systems throughout the organization. However, we were unable to find evidence that the CFPB had

[10] NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations,* Revision 5, updated December 10, 2020, controls CP-2, *Contingency Plans,* and CP-4, *Contingency Plan Testing.*

tested one critical system in nearly 2 years. The CFPB conducted its last successful test of the system in FY 2021.[11]

NIST SP 800-53 Revision 5, control CP-4, Contingency Plan Testing, states, in part:

a. Test the contingency plan for the system
b. Review the contingency plan test results; and
c. Initiate corrective actions, if needed

The lack of documented contingency plan testing for this system may hinder the CFPB's ability to perform mission functions during significant disruptions. Testing the contingency plan will help ensure that the CFPB can effectively restore its business and mission functions and continue performing its mission.

Recommendation
We recommend that the Chief Information Officer (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.

Management Response

The CIO concurs with this recommendation. In his response, the CIO states that the CFPB will develop a report to track when system owners perform tabletop and functional tests in alignment with the now documented role and responsibilities of the system owner. The CFPB will leverage existing governance controls such as the Change Control Board, configuration management, records management, and awareness training to ensure policies and procedures that support contingency planning are included in configurations, tuning, and governance. As the CFPB finalizes its Continuity of Operations Plan (COOP) and Business Continuity approach, it will use this guidance to determine contingency rules in each solution's operational capabilities. The CIO noted that CFPB expects to complete the development of policies and supporting procedures, as well as the contingency plan testing schedule by FY2025 Q4.

Auditor Comment

We believe that the actions described by the CIO are responsive to our recommendations.

[11] CFPB officials indicated that administrative changes prevented the CFPB from performing its annual testing for this contingency plan.

The CFPB Can Update Its Organizational BIA to Support Continuity Planning

The DHS Federal Emergency Management Agency (FEMA) implemented Federal Continuity Directive-2 (FCD-2) to provide direction and guidance to federal executive-branch departments and agencies to validate mission-essential functions (MEFs) to support the organizations' respective contingency planning activities as required by FCD-1. A BIA tests the impact on MEFs in the case of a disruptive event. As such, FCD-2 requires that organizations perform a formal review, update, and validation of their essential functions through a BIA at least every 2 years.[12]

The CFPB has not updated its organizational BIA since 2019, which prevents the CFPB from evaluating its MEFs and determining the impact on its mission if it is unable to perform those functions. This may also prevent the CFPB from creating and maintaining valid and testable Continuity of Operations Plans (COOPs) and Disaster Recovery Plans (DRPs). CFPB officials stated that the CFPB has scheduled a BIA to be completed before the end of the fiscal year.[13] We understand that the CFPB intends to use the updated BIA to guide its contingency planning, as well as to complement existing business continuity plans.

NIST SP 800-34, page 44, paragraph 1, states:[14]

> *Organizations should utilize BIAs to ascertain resiliency and contingency planning strategies. It is essential to evaluate the criticality of a system to missions and assess the potential impact of a system loss.*

Furthermore, NIST SP 800-53, Revision 5, control CP-2, Contingency Plan Testing, states, in part, that the organization:

a. *Identifies essential mission and business functions and associated contingency requirements;*

b. *Provides recovery objectives, restoration priorities, and metrics;*

c. *Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;*

d. *Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;*

Recommendation
We are not making a new recommendation for this finding because it is related to open recommendations 2022-IT-C-014.5 and 2022-IT-C-014.6 from OIG's 2022 Audit of the CFPB's Information Security Program. Additional information is available in Appendix B.

We have included this finding for management consideration.

---

[12] DHS FEMA, Federal Continuity Directive-2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, June 13, 2017.
[13] CFPB officials informed us that the CFPB had updated its MEFs as part of this process, with the intent of submitting of an updated COOP at the end of the project.
[14] NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010.

APPENDIX A: SCOPE AND METHODOLOGY

Cotton & Company Assurance and Advisory, LLC (Cotton), 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 objective. We believe that, based on the objectives of this audit, the evidence obtained through our review of the CFPB's information security program provides a reasonable basis for our findings and conclusions. We carried out our audit planning and testing procedures from March through August 2023.

Our specific audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the CFPB's (1) security controls and techniques for select information systems, and (2) information security policies, procedures, and practices. To accomplish our objectives, we reviewed the effectiveness of the CFPB's information security program across the 20 core metrics and 20 supplemental metrics outlined in OMB's *FY 2023-2024 IG FISMA Reporting Metrics*. These core metrics cover 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 testing activities on the 20 core metrics and 20 supplemental metrics identified in OMB's *FY23 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 level, as well as for three sampled CFPB systems that we selected in coordination with the OIG. We selected the systems to determine the effectiveness of the CFPB's NIST SP 800-53, Revision 5, controls.
    - The OIG based its judgmental selection of the three sampled systems on a risk analysis that it performed on the CFPB's information system inventory. The inventory identified systems by type and mission criticality, as well as whether the systems contained PII.

In previous years, OMB and CIGIE required IGs to use a mode-based scoring approach to assess their agency's maturity levels. Under the mode-based scoring approach, IGs determined the ratings throughout the reporting domains using a simple majority, where the rating that appeared most frequently across the questions (i.e., the mode) served as the domain rating. Through analyses of the data obtained from a pilot program and previous years' IG FISMA reporting, OMB and CIGIE determined that a non-weighted average (i.e., a calculated average) would more closely align with the OIG's assessed maturity levels expressed in a numeric format. Therefore, in FY 2023, IGs must base their ratings on a calculated average approach, where the IG uses the average level of the metrics in a particular domain to determine the effectiveness of the individual function areas (i.e., identify, protect, detect, respond, and recover) and the overall program, with a focus on the core metrics in determining overall maturity. IGs may also consider the following when evaluating maturity:

- The results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing conducted during the review period.
- The progress agencies have made in addressing outstanding IG recommendations.
- Security incidents reported during the review period.

APPENDIX B: STATUS OF PRIOR-YEAR FISMA RECOMMENDATIONS

As part of our FY 2023 FISMA audit, we reviewed the actions that the CFPB had taken to address two outstanding recommendations from prior FISMA audit reports.

Table 2: Status of Open FISMA Recommendations by Security Domain

Year		Recommendation	Status	Explanation
Risk Management				
2017		OIG recommended that CFPB ensure a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.	Open	The CFPB has indicated that it expects to complete this recommendation in FY 2023.
2021	1	OIG recommended that the chief information officer (CIO) continue to work with divisions across the CFPB to develop and implement a cybersecurity risk register and associated process to identify and manage organization-wide cybersecurity risks.	Closed	In FY 2023, the CFPB demonstrated how it used risk register processes at the system, mission, and organization level. The CFPB demonstrated that it aggregates risks from the system level to the organization level and that it communicates risk-based decisions to stakeholders.
2022	3	OIG recommended that the chief information officer (CIO) continue to work with divisions across the CFPB to ensure that policies and supporting procedures for developing and maintaining an enterprise-wide software inventory are developed and maintained.	Open	The CFPB is currently implementing inventory processes to support these procedures.
2022	4	OIG recommended that the chief information officer (CIO) work with divisions across the CFPB to ensure that an enterprise software inventory is conducted and maintained.	Open	The CFPB has demonstrated that it is currently implementing software asset management processes and that it is working toward conducting and managing an enterprise-wise inventory.
Configuration Management				
2014	3	OIG recommended that the chief information officer (CIO) strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.	Open	The CFPB has implemented an application-level scanner. CFPB officials stated that the CFPB has purchased a database security scanning tool but has not yet implemented the tool. The officials estimated that the CFPB will be able to implement the tool into production and begin producing reports against the CFPB's database configurations in the first quarter of 2024. As such, this recommendation will remain open until the CFPB has fully implemented this tool.
2018	1	OIG recommended that the chief information officer (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.	Open	In May 2020, the CFPB updated its vulnerability management process to clarify roles and responsibilities, as well as to document changes to several aspects of its vulnerability management process, including vulnerability disclosure and the monitoring of vulnerabilities introduced by cloud services. The OIG plans to conduct vulnerability scanning to assess the actions that the CFPB has taken to address this recommendation.

Year	Recommendation		Status	Explanation
2021	3	OIG recommended that the chief information officer (CIO) ensure that the CFPB's configuration management plan is updated to reflect current processes, procedures, and technologies.	Closed	In FY 2023, the CFPB provided an updated configuration management plan, which it continues to update regularly. This configuration management plan supports processes to ensure that the CFPB's configuration management practices remain current, such as updating and testing baselines.
Identity and Access Management				
2018	3	OIG recommended that the chief information officer (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	In November 2022, CFPB officials informed us that the CFPB is in the process of implementing a new automated tool to manage these agreements and forms; the officials estimated that the CFPB will finish implementing the tool in the third quarter of 2023. In addition, the CFPB is designing a new privileged user access process; the officials estimated that the CFPB would complete this task by the fourth quarter of 2024.
2019	3	OIG recommended that the chief information officer (CIO) ensure that user-access agreements are consistently utilized to approve and maintain access to CFPB systems for nonprivileged users.	Closed	In FY 2023, the CFPB provided support for closing this recommendation. In particular, the CFPB provided evidence that it had implemented automated processes for approving account access, as well as that it was recording supervisor approvals and was able to provide reports detailing these approvals.
Data Privacy and Protection				
2022	1	OIG recommended that the chief information officer (CIO) ensure that policies and supporting procedures that address data loss prevention configurations, tuning, and governance are developed and implemented.	Closed	In FY 2023, the CFPB provided support for closing this recommendation. In particular, the CFPB provided evidence that it had improved its DLP operational management and governance processes. The CFPB was able to demonstrate that it had documented these DLP processes and that it was monitoring and managing the current DLP mechanisms.
2022	2	OIG recommended that the chief information officer (CIO) ensure that the CFPB's new data loss prevention tool is implemented and configured to monitor traffic across all network access points and environments, as applicable.	Open	The CFPB has indicated that the DLP project is ongoing and that the CFPB is currently implementing DLP protections, including deploying an organization-wide solution.
Contingency Planning				
2022	5	OIG recommended that the chief information officer (CIO) and Administration ensure the development of policies and procedures for the performance and maintenance of an organization-wide business impact analysis.	Open	The CFPB has indicated it has implemented processes and procedures to support the performance and maintenance of an organization-wide BIA.
2022	6	OIG recommended that the chief information officer (CIO) update the CFPB's organization-wide business impact analysis and ensure that the	Open	The CFPB has indicated that it is currently implementing processes to support the creation of an organization-wide BIA by the end of FY 2023.

Year		Recommendation	Status	Explanation
		results are used to make applicable changes to related contingency and continuity plans.		

APPENDIX C: ABBREVIATIONS

BIA	Business Impact Analysis
CDM	Continuous Diagnostic and Mitigation Program
CFPB	Consumer Financial Protection Bureau
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CMDB	Configuration Management Database
COOP	Continuity of Operations Plan
CP	Contingency Plan
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
DLP	Data Loss Protection
DRP	Disaster Recovery Plan
EO	Executive Order
FCD	Federal Continuity Directive
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Planning
MEF	Mission-Essential Function
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SAM	Software Asset Management
SCRM	Supply Chain Risk Management
TIC	Trusted Internet Connection
ZTA	Zero-Trust Architecture

APPENDIX D: MANAGEMENT RESPONSE

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

September 26, 2023

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 *2023 Audit of the CFPB's Information Security Program*. We are pleased that you found the Consumer Financial Protection Bureau's (CFPB) Information Security Program is operating 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) 2024, 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 a continuous annual assessment of core metrics and a biennial assessment of select supplemental metrics. In FY 2023, the OIG leveraged the FISMA audit evaluation methodology and used a risk-based approach to evaluate 20 core metrics and 20 supplemental metrics. The metrics are grouped into nine security domains, which align with the five function areas in the Cybersecurity Framework (*identify, protect, detect, respond, recover*). Furthermore, the draft report states the following and the CFPB offers responses to these statements:

The CFPB is operating at a level 3 maturity (*consistently implemented*) for the **Identify** function.

- In FY 2023, the CFPB's maturity increased from a level 2 (*defined*). The CFPB integrated risk management tools into multiple domains, such as configuration management, information system continuous monitoring, and incident response. Additionally, the CFPB

consumerfinance.gov

is making significant improvements in processes and procedures in risk management and supply chain risk management. In FY2024, the CFPB plans to make progress towards addressing the findings related to developing and maintaining an enterprise-wide software inventory management.

The CFPB is operating at a level 3 maturity (*consistently implemented*) for the **Protect** function.

- In FY 2023, the CFPB's maturity increased from a level 2 (*defined*). The CFPB made considerable progress in the areas of configuration management, identity and access management, data protection and privacy, and security training. In the configuration management domain, the CFPB continued to integrate with the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program, which improves its ability to monitor and manage network operations. In the identity and access management domain, the CFPB expanded its use of phishing-resistant multi-factor authentication (MFA), which further strengthens its authentication mechanisms. In the data protection and privacy domain, the CFPB implemented data privacy processes such as privacy assessments to manage personally identifiable information (PII) and other sensitive information. Finally, in the security training domain, the CFPB maintained a cybersecurity training program that provides training to meet organizational needs while also providing near-real-time adaptive resources to meet user needs. In FY 2024, the CFPB plans to increase our maturity by making continued progress in each respective domain and addressing findings related to data loss prevention.

The CFPB is operating at a level 4 maturity *(managed and measurable)* for the **Detect** function.

- The CFPB's Information System Continuous Monitoring (ISCM) and vulnerability management programs continues to operate effectively at level 4 maturity *(managed and measurable)*. The CFPB's ISCM maintains a continuous assessment program that supports various other programs, such as system authorizations and risk assessment. Additionally, the vulnerability management program remediates issues by maintaining strong communications with business and information technology stakeholders. In FY 2024, the CFPB plans to reach a level 5 maturity (*optimized*) by implementing automated technologies that enable near-real-time control assessments and vulnerability monitoring.

The CFPB is operating at a level 4 maturity *(managed and measurable)* for the **Respond** function.

- The CFPB's incident response program continues to operate at level 4 maturity (*managed and measurable)*. The CFPB maintains an incident ticketing system that assists the incident response teams in responding to incidents identified by various stakeholders and

collaborating with external organizations. Additionally, the CFPB demonstrated its ability to automate incident handling processes by deploying orchestrated incident response technologies. In FY 2024, the CFPB will continue to strengthen its automated technologies, incident communication, and collaboration with internal and external stakeholders to achieve level 5 maturity.

The CFPB is operating at a level 2 maturity (*defined)* for its **Recover** function.

- In FY 2023, the CFPB's maturity decreased from a level 4 (*managed and measurable)*. The CFPB has developed and implemented policies, processes, and procedures for information system contingency plan testing and leveraged lessons learned for future testing. However, the CFPB can improve its ability to adequately respond to disruptive events by implementing consistent contingency planning processes and procedures at the organizational level. In FY 2024, the CFPB plans to address open recommendations related to updating the organization-wide business impact analysis, developing policies and procedures for the performance and maintenance of the organization-wide business impact analysis, and maintaining a comprehensive schedule for testing current contingency plans tracked at the Technology and Innovation level.

We acknowledge that we can improve contingency planning and continue to make progress towards implementing zero-trust architecture requirements. 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,

CHRISTOPHER CHILBERT
Digitally signed by CHRISTOPHER CHILBERT
Date: 2023.09.26 11:55:36 -04'00'

Christopher Chilbert
Chief Information Officer

Response to recommendations presented in the OIG Draft Report: *2023 Audit of the CFPB's Information Security Program*

Recommendation 1: Maintain a comprehensive schedule for testing current contingency plans, documenting test procedures, and maintaining relevant updates to the contingency plan.

Management Response:

The CFPB concurs with this recommendation. The Office of Technology & Innovation (T&I) will develop a report to track when system owners perform tabletop and functional tests in alignment with the now documented role[1] and responsibilities of the system owner. We will leverage existing governance controls such as the CFPB's Change Control Board, configuration management, records management, and awareness training to ensure policies and procedures that support contingency planning are included in configurations, tuning, and governance. As the CFPB finalizes its Continuity of Operations Plan (COOP) and Business Continuity approach, T&I will use this guidance to determine contingency rules in each solution's operational capabilities. We expect to complete the development of policies and supporting procedures, as well as the contingency plan testing schedule by FY2025 Q4.

[1] Information Technology Contingency Planning (ITCP) Training, Testing, and Exercise (TT&E) responsibility, accountability, and authority resides with the respective System Owners. System Owner chain of command reporting is through T&I Directors to the Chief Information Officer (CIO). Accordingly, overall ITCP TT&E reporting responsibility, accountability, and authority resides at the CIO level.