Audit Report
2022-IT-C-014
September 30, 2022

Consumer Financial Protection Bureau

2022 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, 2022-IT-C-014, September 30, 2022

2022 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. Since our review last year, we found that the CFPB has taken steps to strengthen its information security program. For instance, the agency developed its zero trust strategy implementation plan, which outlines the various initiatives and budgetary requirements for the implementation of the CFPB's zero trust architecture (ZTA) by fiscal year 2024. In addition, we found that the CFPB has improved its maturity in the areas of information security continuous monitoring and supply chain risk management.

We identified opportunities to strengthen the CFPB's information security program in the areas of data loss prevention, software asset management, and continuity planning to ensure that its program remains effective. Specifically, we found that the CFPB can strengthen policies and procedures in these areas to ensure that it has repeatable processes in place as it implements its ZTA. We also found that the CFPB can better implement ZTA requirements by ensuring that its new data loss prevention technology is effectively implemented and that an enterprisewide software inventory is developed and maintained. We also found that the CFPB can improve its continuity of operations processes by ensuring that an organizationwide business impact analysis is conducted and maintained.

Finally, the CFPB has taken sufficient actions to close recommendations related to its system authorization and change control processes from our prior Federal Information Security Modernization Act of 2014 (FISMA) audit reports that remained open at the start of this audit. We will update the status of these recommendations in our fall 2022 semiannual report to Congress and continue to monitor the CFPB's progress as part of future FISMA audits.

Recommendations

This report includes six new recommendations designed to strengthen the CFPB's information security program in the areas of data protection and privacy, software asset management, and continuity planning. Our report also includes a matter for management consideration related to the development of procedures for how the CFPB uses a third-party service to monitor vendors' compliance with its cybersecurity requirements. In its response to a draft of our report, the CFPB concurs with our recommendations and outlines actions that have been or will be taken to address them. We will continue to 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 the legislation's 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.

Background

FISMA requires each inspector general 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) fiscal year 2022 guidance for FISMA reporting 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 across several core areas.

These core areas align to requirements outlined in Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance on modernizing federal cybersecurity. The guidance 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, 2022-IT-C-014, September 30, 2022

2022 Audit of the CFPB's Information Security Program

Finding 1: The CFPB Can Strengthen Its DLP Capabilities

Number	Recommendation	Responsible office
1	Ensure that policies and supporting procedures that address DLP configurations, tuning, and governance are developed and implemented.	Office of Technology and Innovation
2	Ensure that the CFPB's new DLP tool is implemented and configured to monitor traffic across all network access points and environments, as applicable.	Office of Technology and Innovation

Finding 2: The CFPB Can Improve Asset Management Processes to Ensure a Comprehensive, Enterprisewide Software Inventory

Number	Recommendation	Responsible office
3	Ensure that policies and supporting procedures for developing and maintaining an enterprisewide software inventory are developed and maintained.	Office of Technology and Innovation
4	Ensure that an enterprisewide software inventory is conducted and maintained.	Office of Technology and Innovation

Finding 3: The CFPB Can Update Its Organizationwide BIA

Number	Recommendation	Responsible office
5	Ensure the development of policies and procedures for the performance and maintenance of an organizationwide BIA.	Office of Technology and Innovation and the Office of Administrative Operations
6	Update the CFPB's organizationwide BIA and ensure that the results are used to make applicable changes to related contingency and continuity plans.	Office of Technology and Innovation and the Office of Administrative Operations

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

MEMORANDUM

DATE: September 30, 2022

TO: Distribution List

FROM: Fred W. Gibson Fred Gibs
Deputy Inspector General

SUBJECT: OIG Report 2022-IT-C-014: *2022 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. To meet our FISMA requirements, we contracted with an independent public accounting firm that assessed the effectiveness of the CFPB's information security program across the core metrics outlined in the Office of Management and Budget's (OMB) *FY22 Core IG Metrics Implementation Analysis and Guidelines*. In addition, this firm also reviewed security controls for select agency systems; the detailed results of this testing will be transmitted in separate memorandums. In addition, we will use the results of this audit to respond to specific questions in OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines*.

We provided you with a draft of our report for 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 D 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
Tiina Rodrigue
Tannaz Haddadi
Marianne Roth
Richard Austin
Ashley Adair

Distribution:
Jean Chang, Acting Chief Operating Officer
Chris Chilbert, Chief Information Officer

Martin Michalosky, Chief Administrative Officer
Ren Essene, Chief Data Officer

Contents

Introduction

Objectives

Our audit objectives, based on the requirements of the Federal Information Security Modernization Act of 2014 (FISMA), were to evaluate the effectiveness of the Consumer Financial Protection Bureau's (1) security controls and techniques for select 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 select systems. To support independent evaluation requirements, the U.S. Department of Homeland Security (DHS), in coordination with the Office of Management and Budget (OMB), publishes FISMA reporting metrics for IGs to respond to on an annual basis.

OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines* focus on 20 key evaluation areas, also known as *core metrics*, that were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance on modernizing federal cybersecurity. These core metrics are detailed in appendix B and cover areas such as

- zero trust architecture (ZTA)[2]
- multifactor authentication and encryption
- investigative and remediation capabilities related to cybersecurity incidents
- endpoint detection and response
- software supply chain security

[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] According to Executive Order 14028, *Improving the Nation's Cybersecurity*, ZTA refers to a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries.

FISMA Maturity Model

OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines* notes that IGs are required to assess the effectiveness of their agencies' information security programs by assessing the core metrics against a maturity model spectrum.[3] The five levels of the maturity model are

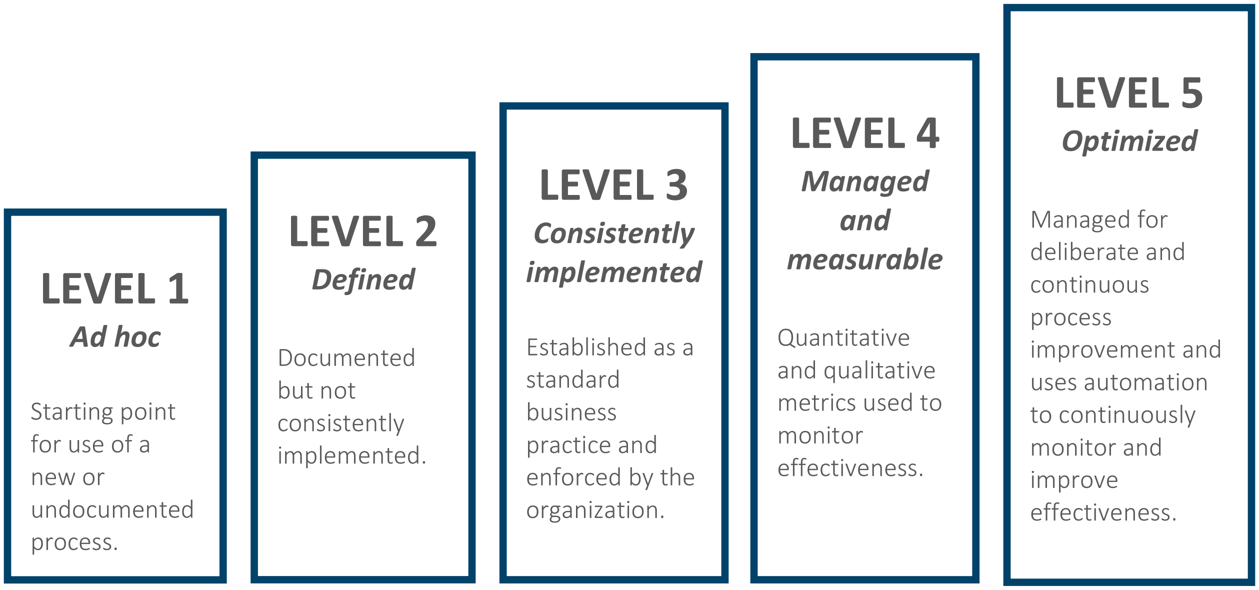
1. *ad hoc*
2. *defined*
3. *consistently implemented*
4. *managed and measurable*
5. *optimized*

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 (figure 1). The maturity levels of each of the core metrics are to be used to determine the overall maturity of an organization's information security program. As noted in OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines*, level 4 (*managed and measurable*) represents an effective level of security.[4] Details on the scoring methodology for the maturity model are included in appendix A.

[3] As noted in the *FY22 Core IG FISMA Metrics Implementation Analysis and Guidelines*, IGs should use the Cyberscope application to submit the results of their core metrics evaluation. As such, our detailed responses and assessment of the CFPB's progress in implementing the core metrics were provided to DHS in the Cyberscope application. Because of the sensitive nature of our responses, they are restricted and not included in this report.

[4] The National Institute of Standards and Technology 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, Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, updated December 10, 2020.

Figure 1. FISMA Maturity Model Rating Scale



LEVEL 1

Ad hoc

Starting point for use of a new or undocumented process.

LEVEL 2

Defined

Documented but not consistently implemented.

LEVEL 3

Consistently implemented

Established as a standard business practice and enforced by the organization.

LEVEL 4

Managed and measurable

Quantitative and qualitative metrics used to monitor effectiveness.

LEVEL 5

Optimized

Managed for deliberate and continuous process improvement and uses automation to continuously monitor and improve effectiveness.

Source: OIG analysis of DHS's *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, May 12, 2021.

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. Since our review last year, we found that the CFPB has taken several steps to strengthen its information security program. For instance, pursuant to the requirements of OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, the CFPB has developed a Zero Trust Strategy Implementation Plan. The plan notes that the agency has incorporated ZTA concepts into its technical guidelines, standards, and architectures since 2019. The agency has also chartered a working group that is tasked with updating the CFPB's near-term and long-term ZTA. Further, we found that the CFPB has started using a federal shared service that provides multifactor authentication support for a select public-facing application.

We identified opportunities for the CFPB to mature its information security program in the areas of data loss prevention (DLP), software asset management (SAM), and continuity planning (CP) to ensure that its program remains effective. We also believe that improvements in the areas of DLP and SAM will better enable the CFPB to meet ZTA requirements.

- Data loss prevention. With respect to DLP, we found that the CFPB uses multiple tools to protect against unauthorized access and transmission of sensitive agency information. However, the agency's transition to a new DLP technology platform has been delayed, and the agency has not developed policies and procedures on DLP configuration, tuning, and governance to ensure a successful implementation of the new technology.
- Software asset management. In the area of SAM, we found that the CFPB performs targeted software inventories of specific technology environments and is piloting a tool as part of the Continuous Diagnostics and Mitigation (CDM) program to help it improve capabilities in this area. However, the agency has not performed a comprehensive, enterprisewide inventory of the software on its network.
- Continuity planning. With respect to CP, we found that the CFPB has not updated its organizationwide business impact analysis (BIA) since 2019. The BIA is a mechanism with which to analyze the potential negative effects of failing to perform an agency's mission-essential functions. The results of the BIA can be used to prioritize response activities and can serve as an input into other continuity plans.

We also noted that the CFPB has not developed procedures for how it will use a third-party service to monitor vendors' compliance with its cybersecurity requirements, and our report includes an item for management consideration in this area. Finally, as highlighted in appendix C, the agency has also taken actions to close recommendations related to the agency's system authorization and change control processes.

Finding 1: The CFPB Can Strengthen Its DLP Capabilities

DLP capabilities are designed to detect and prevent the unauthorized transmission of sensitive information. As noted in OMB Memorandum M-22-09, agencies should strive to employ machine learning to categorize the data they gather and to deploy processes that offer early warning or detection of anomalous behavior in as close to real time as possible throughout their enterprise. DLP technology is one type of tool that can be used to assist an agency in automating security responses in a ZTA. A DLP solution is also recommended for use by federal agencies to monitor personally identifiable information internally and at network boundaries for unauthorized transfers.[5]

The CFPB uses several automated tools to monitor and protect against the unauthorized transmission of sensitive information. This year, we found that the CFPB has decommissioned the use of its current DLP tool, and its migration to a new DLP technology platform has been delayed.[6] CFPB officials notified us that the configuration and implementation of its new DLP tool have been delayed because of staffing changes. In addition, we noted that the CFPB has not developed policies and procedures, as required by National Institute of Standards and Technology, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53, Rev. 5), that outline the specific parameters or thresholds it will use for DLP monitoring, tuning, or governance.[7] CFPB officials notified us that they are relying on the agency's acceptable use policy to serve as a compensating control while they develop supporting DLP policies, procedures, and guidance. CFPB officials also noted that they are awaiting the finalization of the agency's policy on controlled unclassified information to ensure that the implementation of the new DLP tool aligns with these requirements.[8]

We believe that the implementation of the CFPB's new DLP tool and development of supporting policies and procedures on configuration, tuning, and governance will help ensure that sensitive agency information is adequately protected from unauthorized disclosure. Our 2019 FISMA audit report includes a recommendation for the CFPB's chief information officer (CIO) to perform a risk assessment to determine (1) the optimal deployment of the CFPB's technology for monitoring and controlling data

[5] National Institute of Standards and Technology, Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, April 2010; National Institute of Standards and Technology, Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, updated December 10, 2020, control SC-7, *Boundary Protection*.

[6] CFPB officials informed us that the agency does have DLP configured for a specific system that may house data that are classified as controlled unclassified information.

[7] SP 800-53, Rev. 5, control SC-1, *Policy and Procedures*, requires agencies to develop, document, and disseminate policies and procedures to facilitate the implementation of DLP controls.

[8] The National Institute of Standards and Technology notes that controlled unclassified information includes information that the government creates or processes, or that an entity creates or processes for or on behalf of the government, that a law, regulation, or governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, controlled unclassified information does not include classified information or information a non–executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive agency or an entity acting for an agency.

exfiltration to all network access points and (2) appropriate access to internet storage sites.[9] Because the now-decommissioned DLP tool was in use when we made our 2019 recommendation, we are closing this recommendation and issuing a new one related to the CFPB's implementation of its new tool.

Recommendations

We recommend that the CIO, in coordination with the chief data officer,

1. Ensure that policies and supporting procedures that address DLP configurations, tuning, and governance are developed and implemented.

2. Ensure that the CFPB's new DLP tool is implemented and configured to monitor traffic across all network access points and environments, as applicable.

Management Response

The CIO concurs with our recommendations. In his response, the CIO states that the CFPB launched a project in fiscal year 2022 to implement a phased deployment of a new DLP solution. These phases will enable the CFPB to monitor traffic across multiple network access points and environments. The CIO also states that the CFPB will develop and refine policies and procedures to govern the agency's DLP capability and will leverage existing governance controls as part of this process. Further, the CIO notes that the anticipated completion date for the implementation of the DLP solution and supporting policies and procedures is the fourth quarter of fiscal year 2023.

OIG Comment

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

[9] Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*, OIG Report 2019-IT-C-015, October 31, 2019.

Finding 2: The CFPB Can Improve Asset Management Processes to Ensure a Comprehensive, Enterprisewide Software Inventory

As noted in OMB Memorandum M-22-09, a necessary foundation for an enterprisewide ZTA is a complete understanding of the devices, users, and systems interacting within an organization. OMB Memorandum M-22-09 further notes that federal agencies must create ongoing, reliable, and complete asset inventories, including by leveraging DHS's CDM program. Robust software inventory processes can also assist agencies with managing licenses and gaining visibility into their information technology (IT) supply chains.

We found that the CFPB has not established processes to conduct a comprehensive, enterprisewide inventory of the software installed on its network. A key reason for this issue is that while the CFPB conducts targeted inventories for specific technology platforms, it does not have supporting policies and procedures for conducting and maintaining an enterprisewide software inventory. In addition, as noted in its ZTA implementation plan, the agency is in the process of centralizing its software asset inventory information. Further, the CFPB is collaborating with DHS to test and deploy a solution that will automate the discovery and inventorying of IT assets, including software. The CFPB anticipates having this solution fully implemented in fiscal year 2023.

A process to conduct and maintain an enterprisewide software inventory could help ensure that the CFPB is effectively securing the software on its network. A reliable software inventory could also provide valuable information for licensing management purposes and provide a foundation with which to effectively implement CDM tools, in support of the CFPB's ZTA implementation plan.

Recommendations

We recommend that the CIO

3. Ensure that policies and supporting procedures for developing and maintaining an enterprisewide software inventory are developed and maintained.

4. Ensure that an enterprisewide software inventory is conducted and maintained.

Management Response

The CIO concurs with our recommendations. In his response, the CIO states that the CFPB has launched a project to improve the operations of the agency's configuration management database (CMDB) with the goal of providing a complete and accurate repository of CFPB applications, services, and hardware and software inventories. As part of this project, current procedures will be updated to ensure the ongoing maintenance of the CMDB, which is scheduled to be completed by the third quarter of fiscal year 2023. In addition, the CIO states that the CFPB's asset management team will assess, update, and maintain the agency's enterprisewide software repository as the policies and procedures are published. The CIO notes that the next enterprisewide software inventory is scheduled to be completed by the fourth quarter of fiscal year 2023.

OIG Comment

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

Finding 3: The CFPB Can Update Its Organizationwide BIA

Federal agencies, including the CFPB, conduct CP activities to effectively mitigate against threats that may affect mission performance.[10] DHS's Federal Emergency Management Agency has published guidance for the development of continuity programs and planning requirements for executive agencies. Specifically, Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process* (FCD 2) provides direction to assist in the identification of essential functions and the completion of an organizationwide BIA.[11] An organizationwide BIA identifies the potential negative effects of failing to perform a mission-essential function and assists in prioritizing resources. FCD 2 requires federal agencies to review, update, and validate their organization's essential functions by performing a BIA every 2 years.

We found that the CFPB has not updated its organizationwide BIA since 2019.[12] A key reason for this is that the agency has not developed formal policies or procedures detailing how an organizationwide BIA should be conducted, how often it should be updated, and how it should be used in strategy and continuity plan development. CFPB officials also informed us that security resources were devoted to pandemic response activities, resulting in delays. However, these same officials informed us that the agency is in the process of awarding a contract to a third party to perform an organizationwide BIA.

We have made recommendations in previous years' FISMA reports related to strengthening the CFPB's continuity and contingency planning activities that we have since closed based on agency actions. In our 2016 FISMA report, we recommended that the CIO strengthen the agency's contingency program by (1) performing an agencywide BIA and (2) updating the agency's continuity of operations plan and IT contingency plan to reflect the results of the BIA and the current operating environment of the agency.[13] Further, in our 2019 FISMA report, we recommended that the CIO ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.[14] While we have closed these recommendations, we believe that an updated organizationwide BIA can assist the CFPB in ensuring that contingency planning for any of the agency's mission-essential

[10] The Federal Emergency Management Agency's *Continuity Guidance Circular* notes that *CP* refers to the practice of ensuring the execution of essential functions and providing critical services and core capabilities through all circumstances.

[11] FCD 2 defines three types of essential functions: national essential functions, primary mission-essential functions, and mission-essential functions. *National essential functions* are select functions that are necessary to lead and sustain the nation during a catastrophic emergency. *Primary mission-essential functions* are those mission-essential functions that must be continuously performed to support or implement the uninterrupted performance of national essential functions. *Mission-essential functions* are essential functions directly related to accomplishing the organization's mission. U.S. Department of Homeland Security, Federal Emergency Management Agency, Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, June 13, 2017.

[12] The CFPB has determined that it does not have any mission-essential functions that support national continuity.

[13] Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*, OIG Report 2016-IT-C-012, November 10, 2016.

[14] Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*, OIG Report 2019-IT-C-015, October 31, 2019.

functions is prioritized and receives the necessary resources. We also believe that an updated organizationwide BIA can be used to guide contingency planning activities at the information system level.

Recommendations

We recommend that the CIO, in coordination with the chief administrative officer,

5. Ensure the development of policies and procedures for the performance and maintenance of an organizationwide BIA.

6. Update the CFPB’s organizationwide BIA and ensure that the results are used to make applicable changes to related contingency and continuity plans.

Management Response

The CIO concurs with our recommendations. In his response, the CIO states that developing policies and procedures is included in the scope of work for updating the CFPB’s organizationwide BIA, continuity of operations plan, and pandemic plans, via contractor support and based on approved funding. The CIO further notes that the contract is expected to be awarded by the end of fiscal year 2022 and the effort is expected to be completed by the fourth quarter of fiscal year 2023.

OIG Comment

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

Matter for Management Consideration

We identified one matter for management consideration on the development of procedures outlining how the CFPB will use its third-party vendor risk indicator service to continuously monitor vendors' compliance with its cyber supply chain risk management (SCRM) requirements. Because the agency is in the process of updating its SCRM policies and procedures, we are not making a formal recommendation in this area. We will continue to monitor the CFPB's progress in maturing its SCRM program as part of our future FISMA reviews.

The CFPB Can Strengthen Its Procedures for Monitoring Vendors' Compliance With Its Cybersecurity Policies

SCRM, particularly as it relates to information and communications technology, is a risk area across the federal government that has received increased scrutiny. The CFPB has developed a standard operating procedure that outlines the processes the agency uses to manage cybersecurity-related supply chain risks throughout its IT environment as well as the roles and responsibilities with respect to SCRM activities both pre- and postprocurement. The procedure also mentions a third-party vendor risk indicator service that is used to inform the CFPB's SCRM activities. For example, as part of both the pre- and postprocurement phases, the procedure notes that the CFPB uses cybersecurity hygiene and portfolio performance scores for vendors; the scores are provided via this service.

Although the CFPB's standard operating procedure provides a high-level overview of the use of the third-party vendor risk indicator service, the agency has not developed detailed operational procedures to ensure that the use of the service is effectively integrated throughout its SCRM processes. For example, such procedures could outline how to use vendor hygiene and portfolio performance scores and related information and when to reach out to a vendor for additional information. Further, SP 800-53, Rev. 5, notes that agencies should develop procedures that facilitate the implementation of SCRM controls. CFPB officials informed us that that they are in the process of updating their SCRM policies and procedures, and as such, we are not making a recommendation in this area. We will continue to monitor the CFPB's progress in maturing its SCRM processes as part of our future FISMA reviews.

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 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 outlined in OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines*. 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 identified in OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines*
- 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[15]

We contracted with an independent public accounting firm that assessed the effectiveness of the CFPB's information security program across the nine FISMA domains. We reviewed and monitored the work of the contractor to ensure compliance with the contract and *Government Auditing Standards*.

The *FY22 Core IG Metrics Implementation Analysis and Guidelines* directs IGs to assess the effectiveness of information security programs on a maturity model spectrum. In prior years, to rate the maturity of the CFPB's information security program and functional areas, as outlined in the FISMA guidance, we used a scoring methodology determined by a simple majority, where the most frequent level (that is, the mode) across the metrics serves as the overall rating. However, the *FY22 Core IG Metrics Implementation Analysis and Guidelines* notes that an assessment of the 20 core metrics should provide sufficient data to determine the effectiveness of an agency's information security program. Further, the guidance also provides IGs with additional flexibility to use supplemental reports (including past evaluations in which results have varied little from year to year) and any additional evidence of information security program effectiveness to provide context within this evaluation period.

We performed our fieldwork from March 2022 to August 2022. We conducted this 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 we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[15] We plan to transmit the detailed results of our testing of these systems in separate, restricted memorandums because of the sensitive nature of the information.

Appendix B: Core Metrics

The table below shows the 20 core metrics for use in the fiscal year 2022 IG evaluation period. These metrics were selected from the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*[16] for their applicability to critical efforts emanating from Executive Order 14028 and OMB Memorandum M-22-09.[17]

Table B-1. Core Metrics, by Security Domain

Metric title	Metric
Risk management	
System/interconnection inventory	To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems) and system interconnections?
Hardware inventory	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including government-furnished equipment and bring-your-own-device mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?
Software/license inventory	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?
Policies and procedures	To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?
Automated view of risk	To what extent does the organization utilize technology/automation to provide a centralized, enterprisewide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?

[16] U.S. Department of Homeland Security, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, May 12, 2021.

[17] Because of the sensitive nature of the information, the details of our analysis of the *FY22 Core IG Metrics Implementation Analysis and Guidelines*, including the maturity ratings, were provided separately to applicable stakeholders.

Metric title	Metric
Supply chain risk management	
Requirements for external providers	To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?
Configuration management	
Configuration settings	To what extent does the organization utilize settings/common secure configurations for its information systems?
Flaw remediation	To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?
Identity and access management	
Authentication mechanisms (nonprivileged users)	To what extent has the organization implemented strong authentication mechanisms (personal identity verification (PIV) or an identity assurance level (IAL) 3/authenticator assurance level (AAL) 3 credential) for nonprivileged users to access the organization's facilities (organization-defined entry/exit points), networks, and systems, including for remote access?
Authentication mechanisms (privileged users)	To what extent has the organization implemented strong authentication mechanisms (a PIV or an IAL 3/AAL 3 credential) for privileged users to access the organization's facilities (organization-defined entry/exit points), networks, and systems, including for remote access?
Least privilege and separation of duties	To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed.
Data protection and privacy	
Privacy security controls	To what extent has the organization implemented the encryption of data at rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its personally identifiable information and other agency sensitive data, as appropriate, throughout the data life cycle?

Metric title	Metric
Security controls for exfiltration	To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?
Security training	
Assessment of skills, knowledge, and abilities	To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of *identify*, *protect*, *detect*, *respond*, and *recover*?
Information security continuous monitoring	
Information security continuous monitoring (ISCM) policies and strategy	To what extent does the organization utilize ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?
Ongoing system authorizations	How mature are the organization's processes for performing ongoing information system assessments; granting system authorizations, including developing and maintaining system security plans; and monitoring system security controls?
Incident response	
Incident detection and analysis	How mature are the organization's processes for incident detection and analysis?
Incident handling	How mature are the organization's processes for incident handling?
Contingency planning	
BIA	To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts?
Contingency testing	To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Source: OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines*.

Appendix C: Status of Select Prior FISMA Recommendations

As part of our 2022 FISMA audit, we reviewed the actions taken by the CFPB to address select outstanding recommendations from prior FISMA audit reports. We are following up on the status of all outstanding prior FISMA recommendations and will report our results separately. We will update the status of these recommendations in our fall 2022 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.

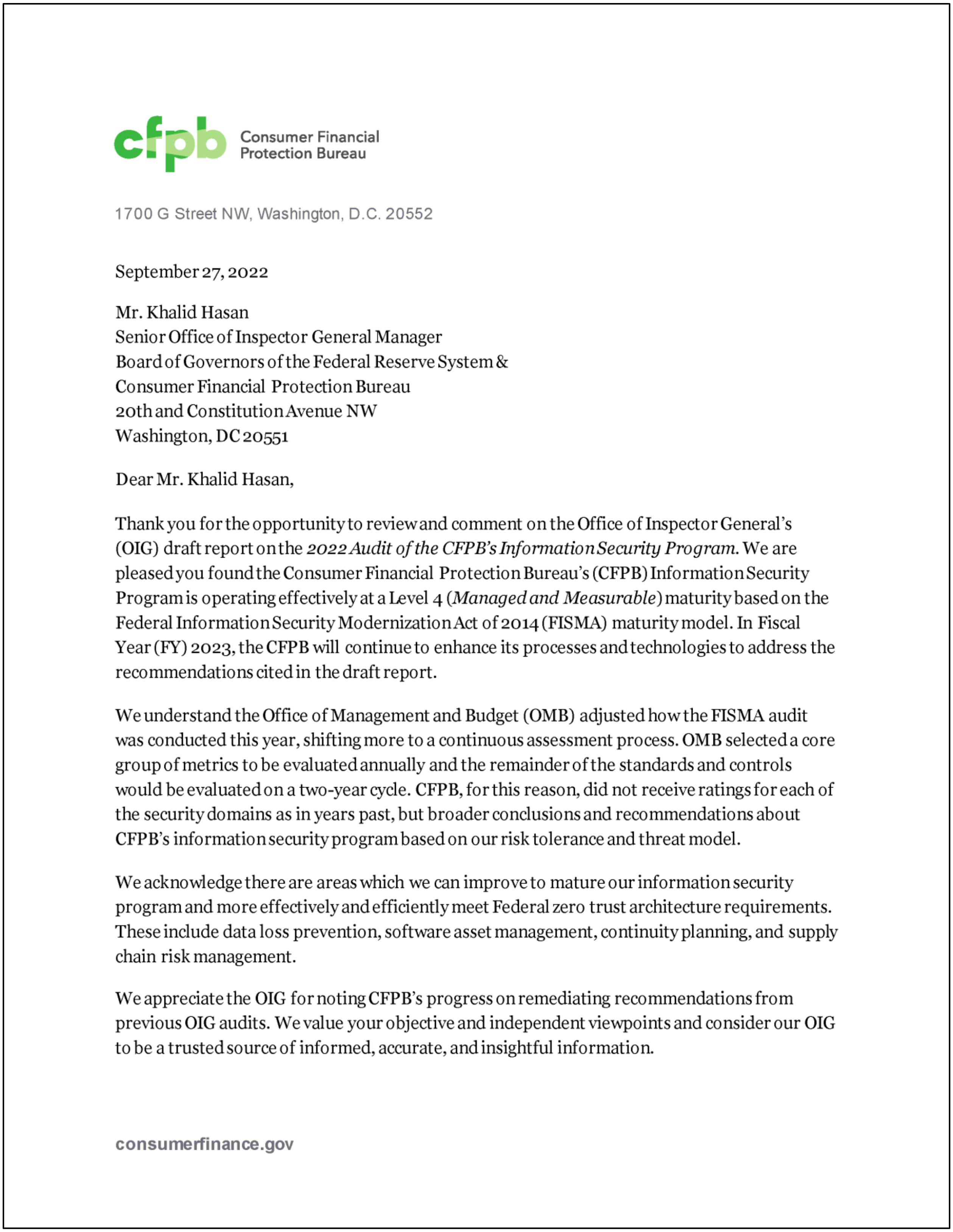
Table C-1. Status of Select FISMA Recommendations That Were Open as of the Start of Our Fieldwork, by Security Domain

Year	Recommendation		Status	Explanation
Risk management				
2019	2	We recommend that the CIO ensure that established security assessment and authorization processes are performed prior to the deployment of all cloud systems used by the CFPB.	Closed	The CFPB took steps to authorize the cloud systems identified in our 2019 FISMA audit report and developed a dashboard to monitor the authorization status of all of the agency's cloud systems.
Configuration management				
2018	1	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.	Pending verification	In May 2020, the CFPB updated its vulnerability management process to clarify roles and responsibilities as well as document changes to several aspects of its vulnerability management process, including vulnerability disclosure and the monitoring of vulnerabilities introduced by cloud services. We plan to conduct vulnerability scanning to verify that configuration-related vulnerabilities are remediated in a timely manner.
2020	1	We recommend that the CIO ensure that (a) change control policies and procedures address separation of duties in the change management life cycle and (b) separation of duties is enforced in the Bureau's change control tool.	Closed	The CFPB has taken steps to update its change control workflow in its automated tool and made improvements to its policies and procedures to enforce separation of duties.

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 is in the process of implementing a new automated tool that will address this recommendation. The tool has been deployed to select privileged users with the agency anticipating full deployment by the end of 2022.
Data protection and privacy				
2019	5	We recommend that the CIO perform a risk assessment to determine (a) the optimal deployment of the Bureau's technology for monitoring and controlling data exfiltration to all network access points and (b) appropriate access to internet storage sites.	Closed	Because the now-decommissioned DLP tool was in use when we made our 2019 recommendation, we are closing this recommendation and issuing a new one in this report related to the CFPB's implementation of its new tool.

Source: OIG analysis.

Appendix D: Management Response



cfpb Consumer Financial
Protection Bureau

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

September 27, 2022

Mr. Khalid Hasan
Senior Office of Inspector General Manager
Board of Governors of the Federal Reserve System &
Consumer Financial Protection Bureau
20th and Constitution Avenue NW
Washington, DC 20551

Dear Mr. Khalid Hasan,

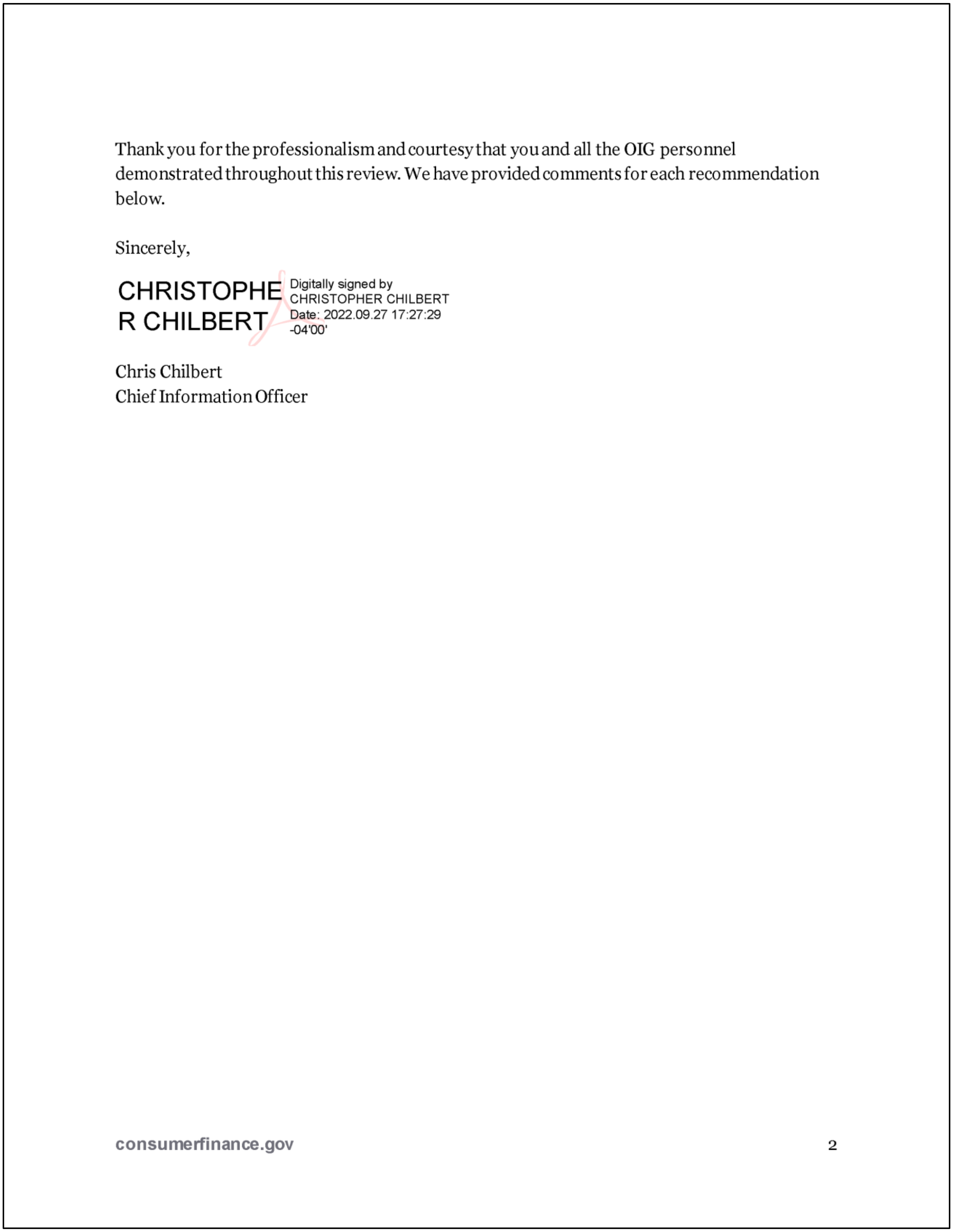
Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the *2022 Audit of the CFPB's Information Security Program*. We are pleased you found the Consumer Financial Protection Bureau's (CFPB) Information Security Program is operating effectively 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) 2023, the CFPB will continue to enhance its processes and technologies to address the recommendations cited in the draft report.

We understand the Office of Management and Budget (OMB) adjusted how the FISMA audit was conducted this year, shifting more to a continuous assessment process. OMB selected a core group of metrics to be evaluated annually and the remainder of the standards and controls would be evaluated on a two-year cycle. CFPB, for this reason, did not receive ratings for each of the security domains as in years past, but broader conclusions and recommendations about CFPB's information security program based on our risk tolerance and threat model.

We acknowledge there are areas which we can improve to mature our information security program and more effectively and efficiently meet Federal zero trust architecture requirements. These include data loss prevention, software asset management, continuity planning, and supply chain 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.

consumerfinance.gov



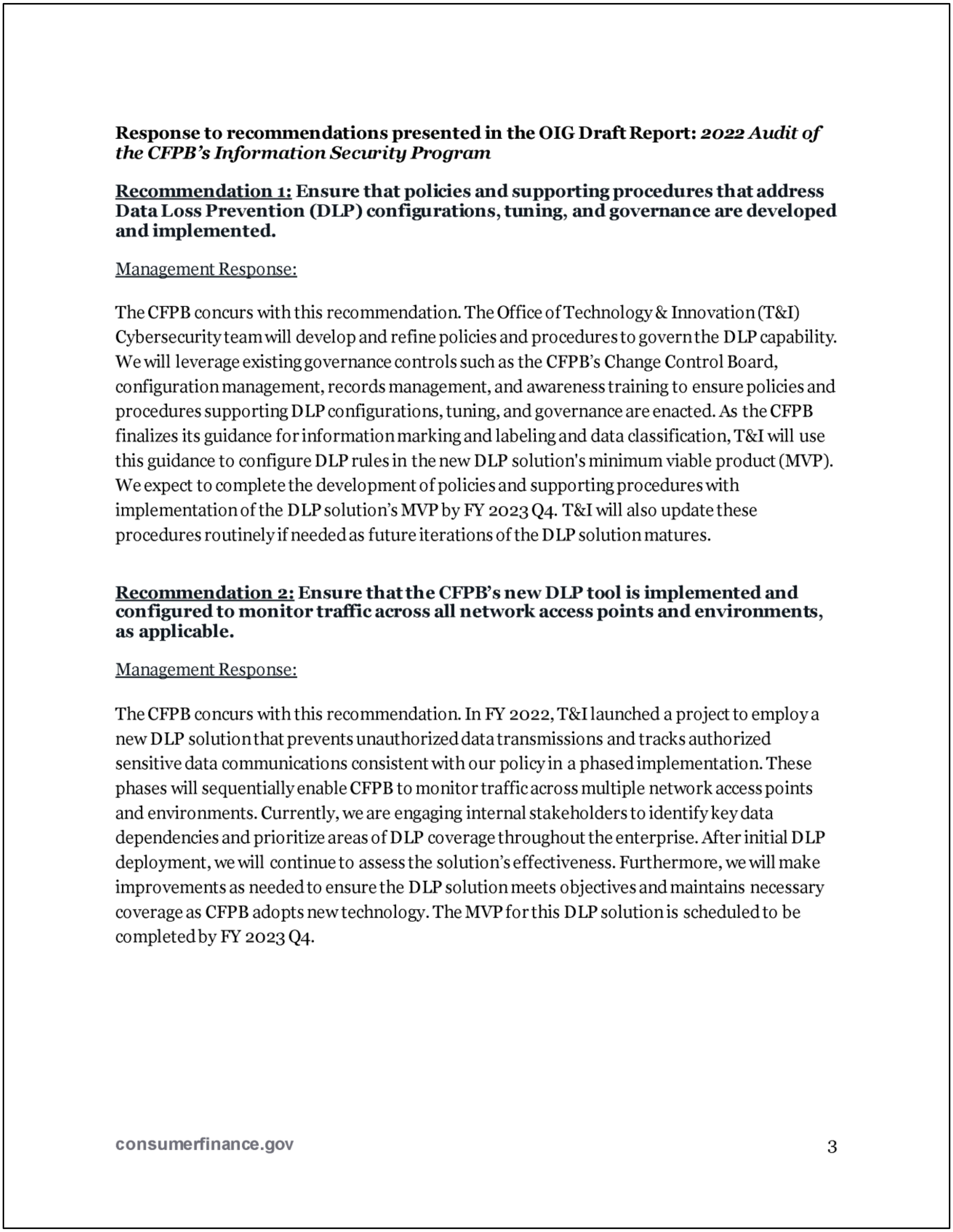
Thank you for the professionalism and courtesy that you and all the OIG personnel demonstrated throughout this review. We have provided comments for each recommendation below.

Sincerely,

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2022.09.27 17:27:29 -04'00'

Chris Chilbert
Chief Information Officer



Response to recommendations presented in the OIG Draft Report: *2022 Audit of the CFPB's Information Security Program*

<u>Recommendation 1:</u> Ensure that policies and supporting procedures that address Data Loss Prevention (DLP) configurations, tuning, and governance are developed and implemented.

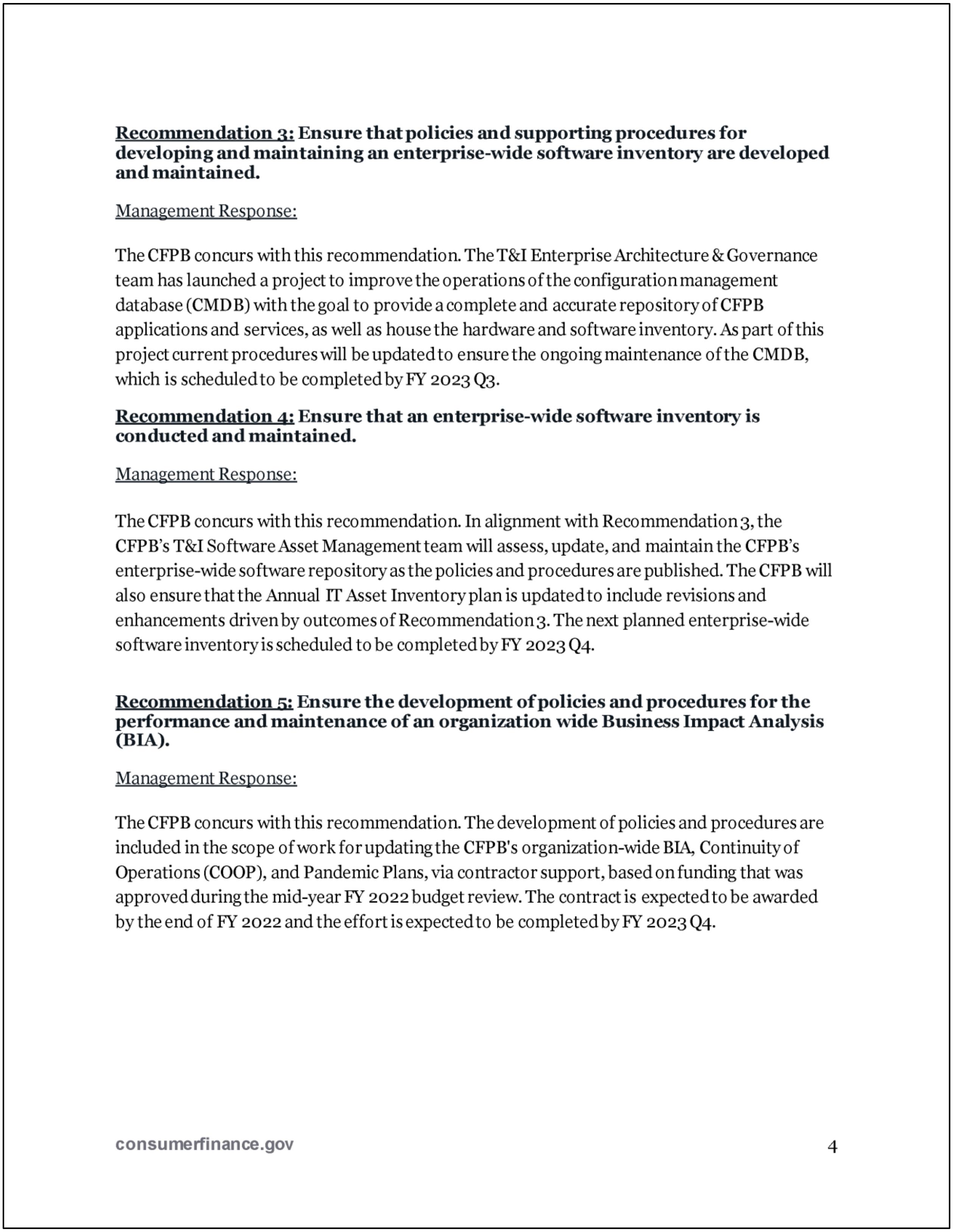
<u>Management Response:</u>

The CFPB concurs with this recommendation. The Office of Technology & Innovation (T&I) Cybersecurity team will develop and refine policies and procedures to govern the DLP capability. 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 supporting DLP configurations, tuning, and governance are enacted. As the CFPB finalizes its guidance for information marking and labeling and data classification, T&I will use this guidance to configure DLP rules in the new DLP solution's minimum viable product (MVP). We expect to complete the development of policies and supporting procedures with implementation of the DLP solution's MVP by FY 2023 Q4. T&I will also update these procedures routinely if needed as future iterations of the DLP solution matures.

<u>Recommendation 2:</u> Ensure that the CFPB's new DLP tool is implemented and configured to monitor traffic across all network access points and environments, as applicable.

<u>Management Response:</u>

The CFPB concurs with this recommendation. In FY 2022, T&I launched a project to employ a new DLP solution that prevents unauthorized data transmissions and tracks authorized sensitive data communications consistent with our policy in a phased implementation. These phases will sequentially enable CFPB to monitor traffic across multiple network access points and environments. Currently, we are engaging internal stakeholders to identify key data dependencies and prioritize areas of DLP coverage throughout the enterprise. After initial DLP deployment, we will continue to assess the solution's effectiveness. Furthermore, we will make improvements as needed to ensure the DLP solution meets objectives and maintains necessary coverage as CFPB adopts new technology. The MVP for this DLP solution is scheduled to be completed by FY 2023 Q4.



<u>Recommendation 3:</u> Ensure that policies and supporting procedures for developing and maintaining an enterprise-wide software inventory are developed and maintained.

<u>Management Response:</u>

The CFPB concurs with this recommendation. The T&I Enterprise Architecture & Governance team has launched a project to improve the operations of the configuration management database (CMDB) with the goal to provide a complete and accurate repository of CFPB applications and services, as well as house the hardware and software inventory. As part of this project current procedures will be updated to ensure the ongoing maintenance of the CMDB, which is scheduled to be completed by FY 2023 Q3.

<u>Recommendation 4:</u> Ensure that an enterprise-wide software inventory is conducted and maintained.

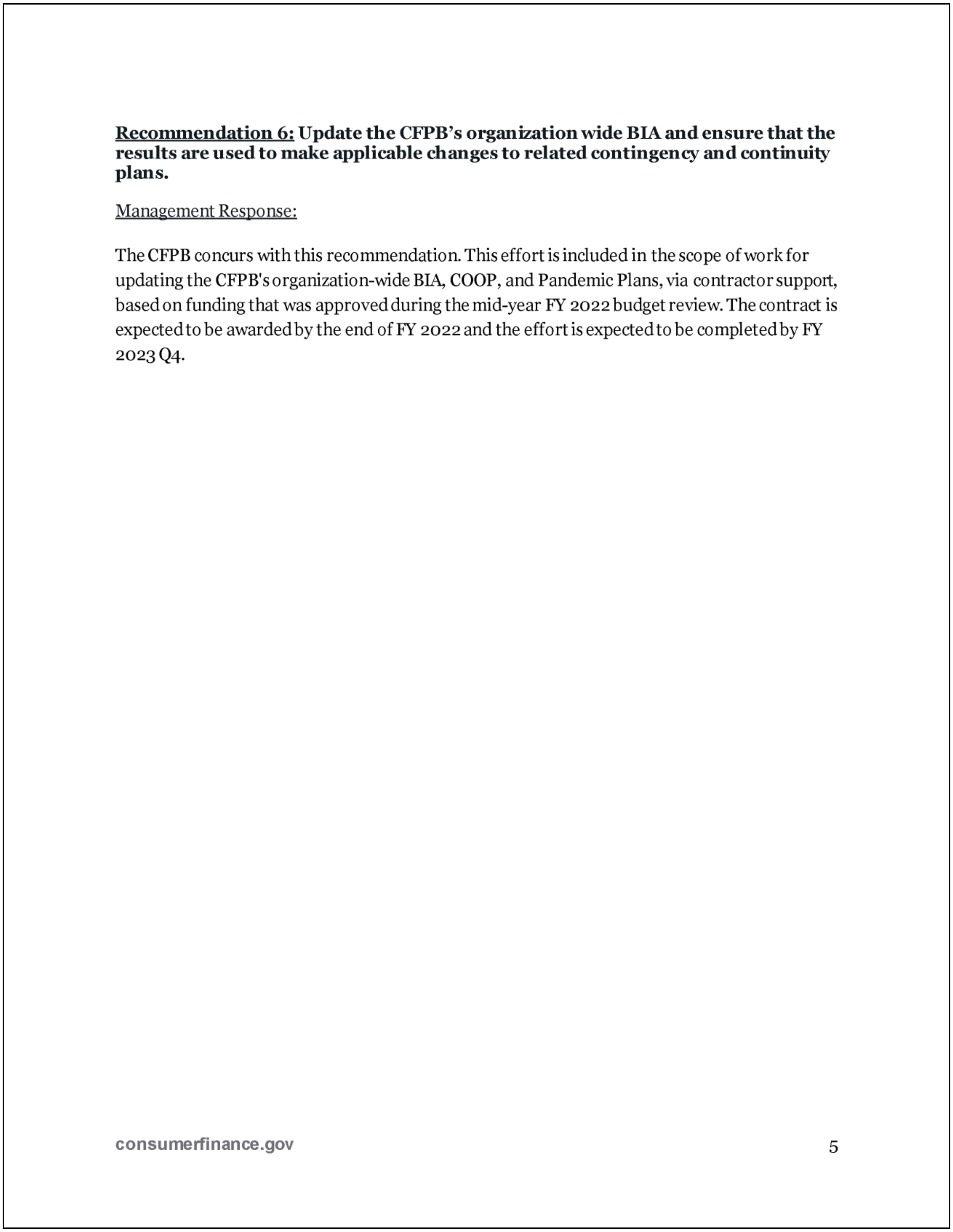
<u>Management Response:</u>

The CFPB concurs with this recommendation. In alignment with Recommendation 3, the CFPB's T&I Software Asset Management team will assess, update, and maintain the CFPB's enterprise-wide software repository as the policies and procedures are published. The CFPB will also ensure that the Annual IT Asset Inventory plan is updated to include revisions and enhancements driven by outcomes of Recommendation 3. The next planned enterprise-wide software inventory is scheduled to be completed by FY 2023 Q4.

<u>Recommendation 5:</u> Ensure the development of policies and procedures for the performance and maintenance of an organization wide Business Impact Analysis (BIA).

<u>Management Response:</u>

The CFPB concurs with this recommendation. The development of policies and procedures are included in the scope of work for updating the CFPB's organization-wide BIA, Continuity of Operations (COOP), and Pandemic Plans, via contractor support, based on funding that was approved during the mid-year FY 2022 budget review. The contract is expected to be awarded by the end of FY 2022 and the effort is expected to be completed by FY 2023 Q4.



<u>Recommendation 6:</u> Update the CFPB's organization wide BIA and ensure that the results are used to make applicable changes to related contingency and continuity plans.

<u>Management Response:</u>

The CFPB concurs with this recommendation. This effort is included in the scope of work for updating the CFPB's organization-wide BIA, COOP, and Pandemic Plans, via contractor support, based on funding that was approved during the mid-year FY 2022 budget review. The contract is expected to be awarded by the end of FY 2022 and the effort is expected to be completed by FY 2023 Q4.

Abbreviations

AAL	authenticator assurance level
BIA	business impact analysis
CDM	Continuous Diagnostics and Mitigation
CIO	chief information officer
CMDB	configuration management database
CP	continuity planning
DHS	U.S. Department of Homeland Security
DLP	data loss prevention
FCD 2	Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*
FISMA	Federal Information Security Modernization Act of 2014
IAL	identity assurance level
IG	inspector general
ISCM	information security continuous monitoring
IT	information technology
OMB	Office of Management and Budget
PIV	personal identity verification
SAM	software asset management
SCRM	supply chain risk management
SP 800-53, Rev. 5	Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
ZTA	zero trust architecture

Report Contributors

Khalid Hasan, Senior OIG Manager for Information Technology
Joshua Dieckert, OIG Manager, Information Technology Audits
Paul Vaclavik, OIG Manager, Information Technology Audits
Ken Dyke, Senior IT Auditor
Chelsea Nguyen, Senior IT Auditor
Nilesh Patel, Senior IT Auditor
Justin Byun, IT Auditor
Aaliyah Clark, IT Auditor
Trang Do, IT Auditor
Melissa Fortson, IT Auditor
Deyanara Gonzalez, IT Auditor
Alexander Karst, Senior Information Technology Management Specialist
Fay Tang, Senior Information Technology Management Specialist
Fred Gibson, Deputy Inspector General

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

OIG

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