Audit Report
2023-IT-C-008
May 31, 2023

Consumer Financial Protection Bureau

Report on the Independent Audit of the CFPB's Agile Systems/Software Development Life Cycle Processes

OIG

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: May 31, 2023

TO: Chris Chilbert
Chief Information Officer
Consumer Financial Protection Bureau

FROM: Khalid Hasan Khalid Hasan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2023-IT-C-008: *Report on the Independent Audit of the CFPB's Agile Systems/Software Development Life Cycle Processes*

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 Agile systems/software development life cycle processes.

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, *Report on the Consumer Financial Protection Bureau's Agile Systems/Software Development Life Cycle Processes*, dated May 24, 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: Adam Martinez
Jean Chang
Tiina Rodrigue
Kathryn Fong
Ren Essene
Dana James
Joshua Galicki
Marianne Roth
Richard Austin
Ashley Adair
Brandi Mix Womack

NONCONFIDENTIAL // EXTERNAL

Cotton

A SIKICH. COMPANY

REPORT ON THE CONSUMER FINANCIAL PROTECTION BUREAU'S AGILE SYSTEMS / SOFTWARE DEVELOPMENT LIFE CYCLE PROCESSES

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

MAY 24 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

May 24 2023

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

Subject: Independent Performance Audit Report on the Consumer Financial Protection Bureau's Agile Systems/Software Development Life Cycle Processes

Cotton & Company Assurance and Advisory, LLC (Cotton), is pleased to submit this independent performance audit report on our audit of the Consumer Financial Protection Bureau's Agile systems/software development life cycle processes. We performed the work from October 2022 through April 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

Cotton

A SIKICH. COMPANY

Executive Summary

Report on the Consumer Financial Protection Bureau's Agile Systems/Software Development Life Cycle Processes

Findings

Cotton & Company Assurance and Advisory, LLC (Cotton), found that the Consumer Financial Protection Bureau's (CFPB's) information security program effectively integrates cybersecurity requirements into its software development life cycle (SDLC) processes while striving to efficiently implement the customer's story, or needs, into its production systems. The CFPB's Office of Technology and Innovation has implemented cloud-based environments that support secure code storage repositories and uses sound development strategies to create and maintain software.

Although the CFPB has effective controls in place, we found that the CFPB can strengthen its policies and procedures to improve its repeatable processes as it strengthens it SDLC program. Specifically, we identified opportunities to strengthen the CFPB's information security program in the areas of privileged user management and software inventory management.

Recommendations

This report includes two findings but no new recommendations, as the CFPB is already in the process of implementing actions for addressing privileged SDLC roles and responsibilities, and a recommendation for improving software inventory management was included in a previous audit. However, the results of our audit do highlight the need for the CFPB to complete its mitigation actions.

Purpose

The objective of the audit was to determine whether the CFPB has effectively integrated the requirements of the Federal Information Security Modernization Act of 2014 (FISMA) into its Agile systems/software development life cycle processes, including using secure software development practices.

Background

FISMA requires federal agencies to ensure that they address information security throughout the life cycle of each of the agency's information systems. In support of FISMA, the Office of Inspector General (OIG) contracted Cotton to conduct an audit to leverage the guidance and definitions in both FISMA and the framework described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.* NIST SP 800-218 recommends that agencies use the Secure Software Development Framework (SSDF), a core set of high-level secure software development practices that agencies can integrate into each SDLC implementation.

Cotton
A SIKICH. COMPANY

Report on the Consumer Financial Protection Bureau's Agile Systems/Software Development Life Cycle Processes

Finding 1: The CFPB Has Not Adequately Defined Roles and Responsibilities for Privileged SDLC Roles

Number	Recommendation	Responsible Office
1	No recommendation is needed, as the CFPB is actively developing relevant policies and procedures for assigning roles in the SDLC.	Office of Technology and Innovation

Finding 2: The CFPB Can Improve Software Component Management Processes with a Comprehensive, Enterprise-wide Software Inventory

Number	Recommendation	Responsible Office
2	No recommendation is needed, as the CFPB is making progress in ensuring that it conducts and maintains an enterprise-wide software inventory.	Office of Technology and Innovation

Cotton
A SIKICH. COMPANY

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Objectives

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the Consumer Financial Protection Bureau (CFPB), to ensure that they (a) address information security throughout the life cycle of their information systems, and (b) integrate information security management processes within their strategic, operational, and budgetary planning processes. FISMA also requires the Office of Inspector General (OIG) to perform an annual independent evaluation of the effectiveness of the agency's information security program, to include testing of security controls for select systems.

In support of these requirements, the OIG for the Board of Governors of the Federal Reserve System and the CFPB contracted Cotton & Company Assurance and Advisory, LLC (Cotton), to conduct an audit of the CFPB's Agile systems/software development life cycle processes. Our objective was to determine whether the CFPB has effectively integrated the requirements of FISMA into its Agile systems/software development life cycle processes, including the use of secure software development practices.

1.2 Background

The President's Executive Order (EO) 14028 on Improving the Nation's Cybersecurity, issued on May 12, 2021, charged multiple agencies—including the National Institute of Standards and Technology (NIST)—with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain. Section 4 of EO 14028 directs NIST to solicit input from the private sector, academia, government agencies, and others and to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security. Those guidelines, which are ultimately aimed at federal agencies but are also available for industry and others to use, include:

- Criteria to evaluate software security.
- Criteria to evaluate the security practices of developers and suppliers.
- Innovative tools or methods to demonstrate conformance with secure practices.

Section 4e of EO 14028 contains ten subsections that each outline actions or outcomes for software producers such as commercial-off-the-shelf product vendors, government-off-the-shelf software developers, and contractors and other custom software developers. To address these requirements, NIST developed Special Publication (SP) 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*. The Secure Software Development Framework (SSDF) is a core set of high-level secure software development practices that can be integrated into each software development life cycle (SDLC) implementation. It is designed to help software producers reduce the number of vulnerabilities in released software, reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. Because the SSDF provides a common vocabulary for secure software development, software acquirers can also use it to foster communications with suppliers in acquisition processes and other management activities.

NIST SP 800-218 defines SDLC as “a formal or informal methodology for designing, creating, and maintaining software (including code built into hardware).” The SP identifies several SDLC models, including Waterfall, Spiral, Agile, and Agile combined with software development and IT operations (DevOps). We briefly describe these models below.

- **Waterfall:** In the Waterfall model, a software development project progresses through a sequence of steps, from initial software concept through maintenance and support. The model is sometimes referred to as document-driven because the organization produces documents in each phase that it then uses in subsequent phases. The documents serve as a progress indicator until a working software product is available.
- **Spiral:** The Spiral model combines the iterative development process model with a sequential linear development model; for example, using the Waterfall model but heavily emphasizing risk analysis. This model allows for incremental releases of the product or incremental refinement through each iteration around the spiral.
- **Agile:** The Agile model also combines the iterative and incremental process models but includes additional focus on process adaptability and customer satisfaction through rapid delivery of working software products. Agile methods break the product into small incremental builds, which the developer provides in iterations. Every iteration involves cross-functional teams working simultaneously on various areas such as planning, requirements analysis, designing, coding, unit testing, and acceptance testing.
- **DevOps:** DevOps is a methodology software development teams use to bring products to market more quickly and efficiently. The DevOps methodology manages the entire software life cycle, from development through release, focusing on collaboration between developers and IT operations professionals. DevOps includes constant software creation, development, verification, release, and management.

In defining the SDLC, NIST SP 800-218 notes that, because few SDLC models explicitly address software security in detail, software developers generally must add and integrate secure software development practices into each SDLC model. Organizations can address most aspects of security multiple times within an SDLC, but in general, the earlier the organization addresses security in the SDLC, the less effort and cost the organization must expend to achieve a given level of security. This principle, known as shifting left, is critical regardless of the SDLC model, as it minimizes any technical debt that would require the organization to remediate early security flaws late in development or after the software is in production.

The CFPB Office of Technology and Innovation (T&I) employs a hybrid version of the Agile and DevOps methodologies. This hybrid methodology includes elements of a predictive approach to development, in which the organization produces a work plan and manages this work plan in an iterative manner throughout the life cycle of the project. The overarching focus of T&I’s hybrid development approach is to prescribe the frequent delivery of high-quality, working software products based on best practices, while also obtaining customer feedback and re-evaluating the product and solution. As such, many CFPB projects are more like configurations than development projects, with the exception of its custom applications; however, even when developing custom applications, T&I uses existing building blocks. Furthermore, many CFPB software projects function in a DevOps environment, in which the development and operations teams are combined into one team, or at least work closely together within their respective technology groups.

1.3 Conclusion

Overall, we found that the CFPB has an effective SDLC process in place, one that uses a DevOps philosophy while integrating Agile processes into the software development and acquisition program. The CFPB's Office of Technology and Innovation has implemented cloud-based environments that support secure code storage repositories and uses sound development strategies to create and maintain software. We further determined that the CFPB's information security program effectively integrates cybersecurity requirements into its SDLC processes while striving to efficiently implement the customer's story, or needs, into its production systems.

Although the CFPB has substantially implemented FISMA requirements into its SDLC processes, we identified opportunities for the CFPB to strengthen its SDLC program in the areas of privileged user policies and software inventories.

1.4 Recommendations

Our report includes two findings that are designed to strengthen the CFPB's SDLC processes. Our audit found that for both areas of weakness, the CFPB had a related finding from a prior-year audit that it was in the process of remediating and/or the CFPB had existing draft procedures it was in the process of approving and implementing. We therefore did not issue any new recommendations.

2. Finding 1: The CFPB Has Not Adequately Defined Roles and Responsibilities for Privileged SDLC Roles

The CFPB has not adequately defined roles and responsibilities for privileged SDLC roles. Specifically, we found:

- The current Acceptable Use Policy (AUP), dated 2016, establishes guidance for CFPB users regarding acceptable and appropriate use of IT resources/systems. However, the AUP does not address privileged SDLC roles, such as software developers.
- The Rules of Behavior (ROB) for Privileged Users, dated 2021, is governed by the AUP and also does not address SDLC roles, such as software developers.

The SSDF recommends that agencies define their cybersecurity requirements and distill those requirements into specific roles that allow secure processes to progress. Agencies must make participants aware of the responsibilities associated with those roles to ensure that software development is both secure and successful. As such, agencies are required to define those roles and support them with appropriate governance.[1] In particular, NIST SP 800-218 directs agencies to define role and responsibility requirements for cybersecurity staff, security champions, project managers and leads, senior management, software developers, software testers, software assurance leads and staff, product owners, operations and platform engineers, and others involved in the SDLC.

Without adequately defining critical roles in the SDLC and related Agile processes, the CFPB could inconsistently manage these roles. This mismanagement could prevent the CFPB from effectively executing its SDLC processes and lead to miscommunication of expectations for SDLC roles and improper performance and evaluation of SDLC-related tasks and responsibilities.

The current Information Security Program Policy (ISPP) is from 2019, and the Acceptable Use Policy (AUP) is from 2016. These policies are dated, and do not reflect subsequent updates in regulations and frameworks, such as the updates to NIST SP 800-53r5 *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-218, and NIST SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. However, we are not issuing a recommendation for this finding, as the CFPB has indicated that it has revised its policies, such as the AUP, and that the updated policies are pending approval. In addition, the CFPB has created draft procedures to document the functions and assignments

[1] NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1*, February 2022, Practice PO.2.1, and NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, updated December 10, 2020, control SA-3, *System Development Lifecyle.*

of SDLC-related roles.[2] We reviewed these draft documents and determined that, if the CFPB implements the draft documents, they would address the above criteria.[3]

3. Finding 2: The CFPB Can Improve Software Component Management Processes with a Comprehensive, Enterprise-wide Software Inventory

The CFPB was not able to provide a comprehensive, enterprise-wide inventory that included software components. The CFPB's different technology groups, such as the Enterprise Platform Team, Infrastructure Team, and Design and Development Team, manage their respective inventories independently, and the CFPB has not completed efforts to centralize the software inventory management process entity-wide. In addition, the separate software inventory lists we received were incomplete and inconsistent. The lack of a comprehensive software inventory, including software components, weakens the CFPB's ability to consistently implement secure software practices.

Accurate and complete software inventories are critical to a successful information security program. Agencies can leverage accurate software inventories to manage and tailor the baselines necessary to ensure the software developed is configured to meet both security and business requirements. Without a sound inventory, agencies will struggle to identify the software assets that should not be installed on their networks. Office of Management and Budget (OMB) Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, requires agencies to inventory software to manage their own software development and to obtain attestation from third parties regarding the security of their software development practices.

CFPB management stated that the CFPB has begun an ongoing effort to improve its software inventory management and reporting process in response to an open audit recommendation from the fiscal year 2022 FISMA audit,[4] which recommended that the CFPB ensure it conducts and maintains an enterprise-wide software inventory. As a result, we are not issuing a recommendation for this finding.

[2] We reviewed the draft policies and procedures and determined that the CFPB based these policies and procedures on updated guidance per NIST SP 800-53, Revision 5, as well as NIST SP 800-218 and NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.*

[3] After the completion of fieldwork, CFPB confirmed that the draft AUP had still not been finalized, however their draft Information Security Program Policy, which was also undergoing updates during the audit, had been finalized and was provided for courtesy review.

[4] https://oig.federalreserve.gov/reports/CFPB-information-security-program-sep2022.pdf

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 Consumer Financial Protection Bureau's (CFPB's) Agile software development life cycle (SDLC) program provides a reasonable basis for our findings and conclusions.

We carried out our audit planning and testing procedures from October 2022 through April 2023. We based our audit scope and methodology on National Institute of Standards and Technology (NIST) Special Publication (SP) 200-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*; the Federal Information Security Modernization Act of 2014 (FISMA); the President's Executive Order (EO) 14028 on Improving the Nation's Cybersecurity; and Office of Management and Budget (OMB) Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.

Our audit reviewed numerous offices and information technology activities within the CFPB. We interviewed personnel associated with the CFPB's SDLC processes, as well as key personnel from various offices, including the Chief Information Security Officer, Cybersecurity Program Management, Security Architecture and Engineering, Infrastructure Solutions, Enterprise Data and Analytics, Cybersecurity Operations, Enterprise Platform Team, Design and Development, and the Chief Privacy Officer.

Based on these interviews, we were informed that the major software development projects at CFPB were divided amongst three primary technology stacks. This was also consistent with documentation we received when reviewing a list of software development projects at CFPB. Therefore, out of the universe of all CFPB systems, we judgmentally selected three systems to review during the audit which covered each of the technology stacks' primary platforms. We obtained and evaluated available documentation related to the CFPB's SDLC program, including existing governance and directives, relevant risk assessments, recent audits and process reviews, training records, configuration settings and tool-generated artifacts (e.g., workflows, issue tracking, mappings), access control lists, network and system architecture documents, software source code management, code execution and configuration controls, the use of cryptographic hashes, certificate management, code signing, and software integrity verification information.

We based our evaluation of CFPB's Agile software development process on the four practice areas identified within the NIST Secure Software Development Framework (SSDF). These four practice areas include:

1. **Prepare the Organization (PO):** Organizations ensure that people, processes, and technology are prepared to perform secure software development at the organizational level.

2. **Protect the Software (PS):** Organizations should protect all components of their software from tampering and unauthorized access.
3. **Produce Well-Secured Software (PW):** Organizations should produce well-secured software with minimal security vulnerabilities in their releases.
4. **Respond to Vulnerabilities (RV):** Organizations should identify residual vulnerabilities in their software releases and respond appropriately to address those vulnerabilities and prevent similar ones from occurring in the future.

We performed these activities to evaluate the overall effectiveness of the CFPB's SDLC program and its compliance with applicable CFPB and federal IT requirements.

APPENDIX B: ABBREVIATIONS

AUP	Acceptable Use Policy
CFPB	Consumer Financial Protection Bureau
Cotton	Cotton & Company Assurance and Advisory, LLC
DevOps	Development and IT Operations
EO	Executive Order
FISMA	Federal Information Security Modernization Act of 2014
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SDLC	Software Development Life Cycle
SP	Special Publication
SSDF	Secure Software Development Framework v 1.1
T&I	Office of Technology & Innovation