



OFFICE OF INSPECTOR GENERAL

Audit Report

2012-AA-C-002

2012 Audit of the
Consumer Financial Protection Bureau's
Information Security Program

November 15, 2012

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Khalid Hasan, OIG Manager

Joshua Dieckert, Auditor-in-Charge

Paul Vaclavik, IT Auditor

Ed Fernandez, Auditor

Peter Sheridan, Senior OIG Manager

Andrew Patchan Jr., Associate Inspector General for Audits and Attestations

Abbreviations

CFPB	Consumer Financial Protection Bureau
FISMA	Federal Information Security Management Act of 2002
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SP 800-53	Special Publication 800-53, Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>
Treasury	Department of the Treasury



Executive Summary:

2012 Audit of the Consumer Financial Protection Bureau's Information Security Program

2012-AA-C-002

November 15, 2012

Purpose

To meet our annual Federal Information Security Management Act of 2002 (FISMA) reporting responsibilities, we reviewed the information security program and practices of the Consumer Financial Protection Bureau (CFPB).

Background

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program. FISMA also requires each agency inspector general to conduct an annual independent evaluation of its agency's information security program and practices.

Findings

Overall, we found that the CFPB has taken several steps to develop, document, and implement an information security program. For example, the CFPB has drafted agency-wide information security and acceptable use policies, as well as procedures for continuous monitoring and risk management. In addition, the CFPB has developed an inventory of FISMA-reportable systems and a baseline of security controls for its information systems. However, we found that additional steps are needed to fully develop, document, and implement an information security program that is consistent with FISMA.

Recommendations

We recommend that the Chief Information Officer develop and implement a comprehensive information security strategy that identifies specific goals, objectives, milestones, and resources to establish a FISMA-based information security program; finalize the agency-wide information security policy and develop procedures to facilitate the implementation of the policy; and analyze the CFPB's contractor oversight processes and information security controls for additional contractor-operated systems and take actions, as necessary, to ensure that FISMA and CFPB information security requirements are met.

Management's Response

In comments to a draft of our report, the CFPB Chief Information Officer concurred with our recommendations and outlined actions that have been taken, are underway, and planned to strengthen CFPB's information security program.

Access the full report: http://www.federalreserve.gov/oig/oig_rpt_2012.htm

For more information, contact the OIG at 202-973-5000 or visit <http://www.consumerfinance.gov/oig>.

Summary of Recommendations, Report No. 2012-AA-C-002

Rec. no.	Report page no.	Recommendation	Responsible office
1	5	Develop and implement a comprehensive information security strategy that identifies specific goals, objectives, milestones, and resources to establish a FISMA-based information security program.	Office of the Chief Information Officer
2	5	Finalize the CFPB's agency-wide information security policy and develop procedures to facilitate the implementation of the policy.	Office of the Chief Information Officer
3	5	Analyze the CFPB's contractor oversight processes and information security controls for additional contractor-operated systems and take actions, as necessary, to ensure that FISMA and CFPB information security requirements are met.	Office of the Chief Information Officer



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

November 15, 2012

MEMORANDUM

TO: Chris Willey
Chief Information Officer, Consumer Financial Protection Bureau

FROM: Andrew Patchan Jr. *Andrew Patchan Jr.*
Associate Inspector General for Audits and Attestations

SUBJECT: *OIG Report: 2012 Audit of the Consumer Financial Protection Bureau's Information Security Program*

The Office of Inspector General (OIG) of the Consumer Financial Protection Bureau (CFPB) is pleased to present the results of our audit of the CFPB's information security program. As the CFPB continues to enhance its information security program, we are providing three recommendations that we believe will further strengthen the CFPB's efforts to meet Federal Information Security Management Act of 2002 requirements.

We provided a draft of our report to you for review and comment. In your response, included as appendix A, you concurred with our recommendations and outlined actions that have been taken, are underway, and planned to strengthen CFPB's information security program. As part of our audit, we also reviewed security controls for a contractor-operated system. The results of our review of security controls for this system will be transmitted under separate, restricted cover. In addition, we will utilize the results of our review of the CFPB's information security program and practices to respond to specific questions in the Department of Homeland Security's FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics. We appreciate the cooperation we received from the CFPB during our review. Please contact me if you would like to discuss this report or any related issues.

cc: Victor Prince, Chief Operating Officer, CFPB
Zach Brown, Chief Information Security Officer, CFPB
Marla A. Freedman, Assistant Inspector General for Audit, Office of Inspector General,
Department of the Treasury
Mark Bialek, Inspector General
J. Anthony Ogden, Deputy Inspector General

Contents

Introduction	1
Objectives.....	1
Background	1
Findings	3
Comprehensive Strategy Should Be Developed to Implement a FISMA-based Information Security Program	3
Information Security Policy Should Be Finalized and Implementing Procedures Developed	4
Information Security Oversight Should Be Strengthened for Contractor-operated Systems.....	4
Recommendations	5
Management’s Response	5
Appendix A—Management’s Response	6
Appendix B—Scope and Methodology	9

Introduction

Objectives

Our specific audit objectives, based on the Federal Information Security Management Act of 2002 (FISMA), were to evaluate the effectiveness of the Consumer Financial Protection Bureau's (CFPB's) security controls and techniques and CFPB's compliance with FISMA and related information security policies, procedures, standards, and guidelines. Our scope and methodology are detailed in appendix A.

Background

FISMA provides a framework for ensuring the effectiveness of information security controls over federal operations and assets and a mechanism for oversight of federal information security programs.¹ FISMA requires agencies to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source. Agency information security programs must provide for, among other things, periodic risk assessments, policies and procedures based on the risk assessments, periodic testing and evaluation of the effectiveness of policies and procedures, security planning, security awareness training, and continuity of operations. FISMA also requires each agency inspector general to perform an annual independent evaluation of the information security program and practices of its respective agency to determine the effectiveness of such program and practices.

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 created the CFPB and charged it with the responsibility of regulating the offering and provisioning of consumer financial products and services.² The CFPB formally began operations in July 2011 with a central mission of making markets for consumer financial products and services work for Americans. The CFPB has established an Office of the Chief Information Officer, which is responsible for the implementation and maintenance of an agency-wide information security program.

In our 2011 FISMA audit report, we noted that as the CFPB began operations, it was relying on the information security program and systems of the Department of the Treasury (Treasury). Since then, the CFPB has begun to develop its agency-wide information security program using the National Institute of Standards and Technology (NIST) Risk Management Framework as a model.³ As part of this approach, the agency is developing processes to

1. Title III, Pub. L. No. 107-347 (December 17, 2002).

2. Pub. L. No. 111-203, Title X, 124 Stat. 1955 (July 21, 2010).

3. NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

promote near real-time risk management and on-going system authorization. The CFPB is also leveraging shared services and cloud computing with the objective of balancing risk, cost, and desired functionality. In addition, the CFPB continues to rely on Treasury for certain information security services, including those for remote access, configuration management, incident response, and identification and authentication.

Findings

Overall, we found that the CFPB has taken several steps to develop, document, and implement an information security program. For example, the CFPB has drafted agency-wide information security and acceptable use policies, as well as procedures for continuous monitoring and risk management. In addition, the CFPB has developed an inventory of FISMA-reportable systems and a baseline of security controls for CFPB information systems. However, we found that additional steps are needed to fully develop, document, and implement an information security program that is consistent with FISMA.

Comprehensive Strategy Should Be Developed to Implement a FISMA-based Information Security Program

The CFPB has not established a comprehensive information security strategy to guide the implementation of an agency-wide information security program. CIO officials stated that this strategy has not been developed because the agency has been focused on formalizing organizational structures and achieving operational capabilities. In addition, an adequate information security strategy should align with CFPB organizational and business level strategies, which are still being developed. The CFPB has issued a draft strategic plan for 2013–2018 outlining its goals, desired outcomes, performance measures, and performance indicators at the organizational level. To promote transparency, the agency has asked the public for comments and feedback on the plan.

NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, recommends as a best practice that federal organizations establish a comprehensive strategy to enable the development, institutionalization, assessment, and improvement of an agency-wide information security program. The strategy should be documented in an information security strategic plan and include a high-level plan for achieving information security goals and objectives, including short- and mid-term objectives and performance targets.

In the absence of an information security strategy, the CFPB's efforts to implement an agency-wide information security program may not adequately align with the goals and needs of the agency. As the CFPB continues to enhance its information security program, we recommend that the Chief Information Officer (CIO) develop and implement a comprehensive information security strategy that identifies specific goals, objectives, milestones, and resources to establish a FISMA-based information security program.

Information Security Policy Should Be Finalized and Implementing Procedures Developed

The CFPB has developed a draft agency-wide information security policy that delineates roles and responsibilities and specifies minimum information security controls for all agency systems. The CFPB has also developed draft procedures for continuous monitoring and risk management. While we found that the Chief Information Officer was performing several FISMA-based information security activities, the CFPB's agency-wide information security policy and procedures were not finalized. CIO officials stated that the agency was focused on formalizing organizational structures and achieving operational capabilities. As such, it had not prioritized the completion of agency-wide information security policy and procedures.

FISMA requires that an agency's information security program include policies and procedures that (1) are based on risk assessments, (2) cost effectively reduce information security risks to an acceptable level, and (3) ensure that information security is addressed throughout the life cycle of each agency information system. In addition, NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (SP 800-53), recommends that information security policies address purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance. SP 800-53 also recommends the development of formal, documented procedures to facilitate the implementation of the policies.

As a result of the lack of an agency-wide information security policy and procedures, we found inconsistent information security processes, undefined roles and responsibilities, and limited documentation to support risk-based decisions. In addition, we identified a contractor-operated system that did not meet a number of FISMA and NIST requirements. As such, we recommend that the CIO finalize the CFPB's agency-wide information security policy and develop procedures to facilitate the implementation of the policy.

Information Security Oversight Should Be Strengthened for Contractor-operated Systems

The CFPB utilizes a number of contractor-operated systems, including several that are hosted in a cloud environment. As part of its contractor oversight process, the CFPB performs security assessments and receives periodic security updates for contractor-operated systems. For a contractor-operated system that we reviewed, we found that the CFPB needs to improve its oversight process to ensure that FISMA requirements are met. We identified a number of management, operational, and technical control weaknesses for this system.⁴ According to CIO officials, these weaknesses existed primarily because the CFPB did not have enough staff to effectively monitor the contractor's compliance with FISMA requirements.

FISMA requires agencies to provide information security controls for information systems used or operated by an agency, including those provided by a contractor of an agency. In addition, SP 800-53 requires organizations to define and document government oversight and user roles and responsibilities regarding external information security services as well as monitor security control compliance by external service providers.

4. The results of our review of the contractor-operated system will be transmitted under separate, restricted cover.

Based on the weaknesses we identified, the CFPB has limited assurance that FISMA and CFPB information security requirements are being met for the contractor-operated system that we reviewed. We will provide the results of our review of this system and specific recommendations under separate, restricted cover. Based on our findings regarding this system, we recommend that the CIO analyze the CFPB's contractor oversight processes and information security controls for additional contractor-operated systems and take actions, as necessary, to ensure that FISMA and CFPB information security requirements are met.

Recommendations

We recommend that the Chief Information Officer:

1. Develop and implement a comprehensive information security strategy that identifies specific goals, objectives, milestones, and resources to establish a FISMA-based information security program.
2. Finalize the CFPB's agency-wide information security policy and develop procedures to facilitate the implementation of the policy.
3. Analyze the CFPB's contractor oversight processes and information security controls for additional contractor-operated systems and take actions, as necessary, to ensure that FISMA and CFPB information security requirements are met.

Management's Response

In comments to a draft of our report, included as appendix A, the CFPB Chief Information Officer concurred with our recommendations and outlined actions that have been taken, are underway, and planned to strengthen CFPB's information security program.

Appendix A

Management's Response



1700 G Street NW, Washington, DC 20552

November 9, 2012

Mr. Andrew Patchan, Jr.
Associate Inspector General for Audits and Attestations
Board of Governors of the Federal Reserve System &
Consumer Financial Protection Bureau
20th and C Streets, NW
Washington, DC 20551

Dear Mr. Patchan,

Thank you for the opportunity to review and comment on the Office of Inspector General's draft report of the *2012 Audit of the Consumer Financial Protection Bureau's Information Security Program*.

We are pleased that you found that the Bureau has taken several steps to develop, document, and implement an information security program, including drafting agency-wide information security and acceptable use policies, as well as developing procedures for continuous monitoring and risk management. We are also pleased that you noted CFPB's development of an inventory of FISMA-reportable systems and a baseline of security controls for its information systems.

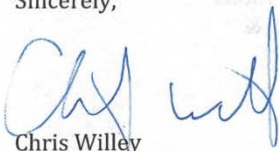
We have reviewed the recommendations that you have provided regarding a comprehensive strategy, an agency-wide information security policy and procedures, and a contractor-operated system. We concur with your draft recommendations.

The information in your draft report addresses CFPB's information security program as of September 30, 2012. Through coordination with your staff, and an understanding of the matters identified in this audit, the Bureau has already begun to take action on the draft recommendations. Such actions include continued progress toward finalizing and implementing policies and procedures, working closely with and providing oversight of our service providers, and monitoring the timely correction of identified errors.

consumerfinance.gov

Thank you again for the opportunity to comment on the report. We provide the following comments for each recommendation.

Sincerely,



Chris Willey
Chief Information Officer

Enclosure

**The Consumer Financial Protection Bureau's Response to Recommendations in
the Draft Report, 2012 Audit of the Consumer Financial Protection Bureau's
Information Security Program**

Recommendation 1: Develop and implement a comprehensive information security strategy that identifies specific goals, objectives, milestones, and resources to establish a FISMA-based information security program.

Response: Management concurs with this recommendation. The CFPB has developed a FISMA-based information security program that aligns to the operational needs and current strategic direction for the Bureau. As a new agency, we have undertaken a strategic planning process for the Bureau as a whole and intend to align division resources to that plan. The CFPB posted a draft of its strategic plan for years 2013-2018 on its website and asked for public comments by October 25, 2012. The plan is expected to be finalized at the beginning of 2013. In the interim, the CFPB Chief Information Officer has also developed a draft strategic plan designed to address the fulfillment of technology and data needs of the Bureau. This CIO Strategic Plan includes a high level plan for the Bureau's information security program and will be complemented by a targeted plan for CFPB information security.

Recommendation 2: Finalize the CFPB's agency-wide information security policy and develop procedures to facilitate the implementation of the policy.

Response: Management concurs with this recommendation. The CFPB is in the final stages of fully documenting and approving its Information Security Policy. The program policy will be complemented by additional policies and procedure documents that exist as operational drafts. Since the CFPB was launched on July 21, 2011, the CFPB has made considerable progress in developing key policies and procedures to carry out its mission. These documents will guide the continued implementation and maturation of the CFPB information security program.

Recommendation 3: Analyze the CFPB's contractor-oversight processes and information security controls for additional contractor-operated systems and take actions, as necessary, to ensure that FISMA and CFPB information security requirements are met.

Response: Management concurs with this recommendation. As the CFPB continues to grow toward its steady-state level of operations, we will continue to analyze contractor-operated systems and strengthen them, as necessary, to ensure that we meet FISMA and CFPB information security requirements. CFPB understands the importance of these issues and will continue to design oversight processes and controls that best support this as a priority.

Appendix B

Scope and Methodology

To accomplish our audit objectives, we reviewed the CFPB's program-level information security policies and procedures, analyzed system security documentation, met with CFPB information security officials and contractors, and observed and tested specific system controls. We also reviewed the CFPB's information security policies, procedures, and controls for a select contractor-operated system listed on the CFPB's FISMA inventory. Our audit scope did not include a review of information security controls for Treasury information systems used by the CFPB.

We conducted our fieldwork from July 2012 to October 2012 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.

As noted, the CFPB relies on certain security services that are part of Treasury's information security program. These services include remote access, configuration management, incident response, and identification and authentication. As part of our response to the Department of Homeland Security's FISMA reporting questions for inspectors general, submitted under separate cover, we relied on the work performed by the Treasury OIG, as part of its FISMA review of Treasury's information security program, for these services. We performed sufficient, appropriate procedures to meet generally accepted government auditing standards requirements for relying on the work of the Treasury OIG, including the following:

- We obtained evidence on the qualifications and independence of contractor staff performing the FISMA audit of Treasury for the Treasury OIG.
- We reviewed Treasury OIG's FISMA audit plan, audit report, and work paper documentation.
- We met with Treasury OIG officials to gain an understanding of how they performed their FISMA oversight of Treasury's information security program, including reviewing the work performed by contractor staff.
- We discussed the contractor's audit approach and results with contractor staff.



OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the
OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig

