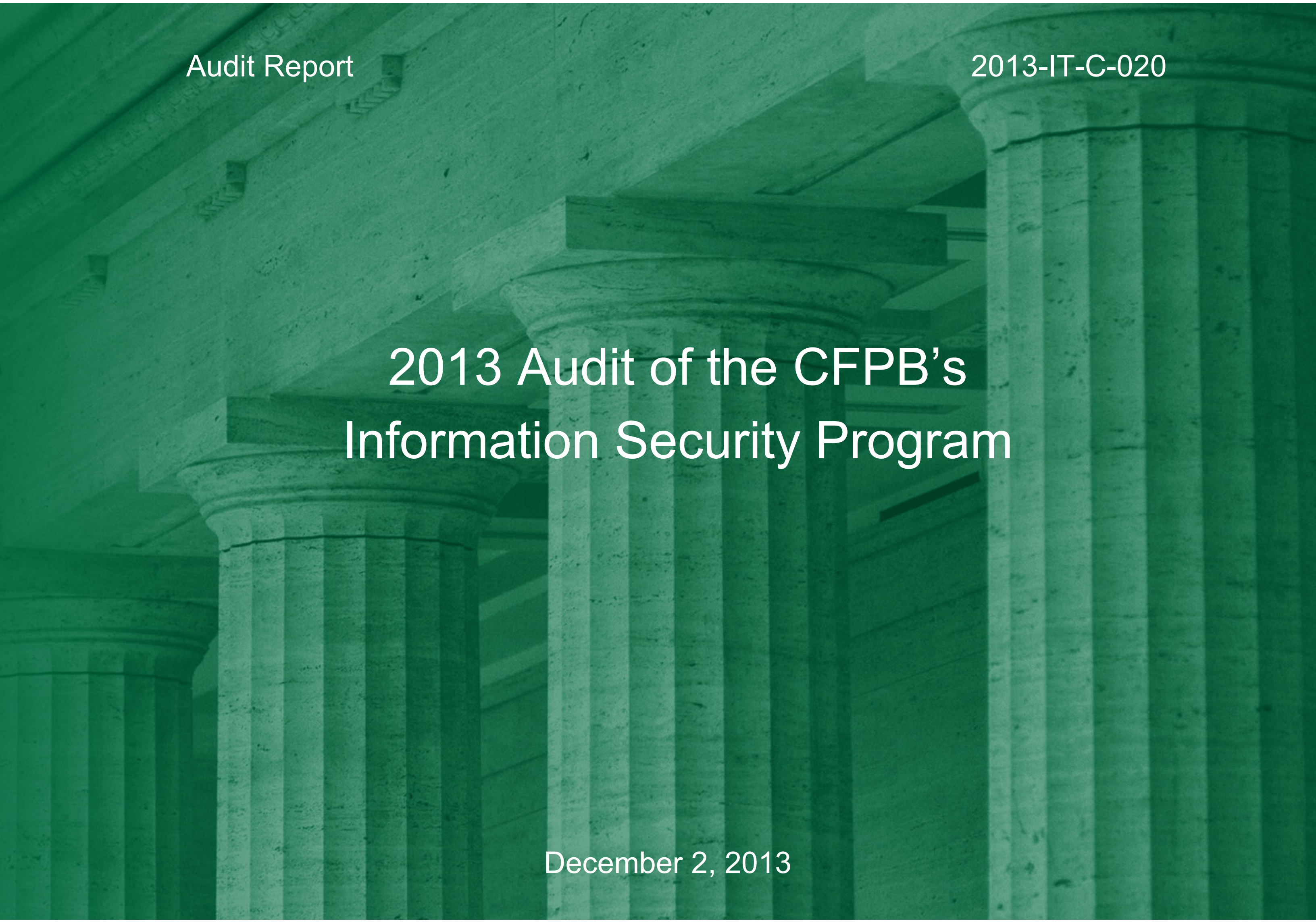
Office of Inspector General



Audit Report

2013-IT-C-020

2013 Audit of the CFPB's Information Security Program

December 2, 2013

Board of Governors of the Federal Reserve System

Consumer Financial Protection Bureau

Report Contributors

Khalid Hasan, OIG Manager
Joshua Dieckert, Auditor-in-Charge
Adam Raley, IT Auditor
Paul Vaclavik, IT Auditor
Peter Sheridan, Senior OIG Manager for Information Technology Audits
Andrew Patchan Jr., Associate Inspector General for Information Technology

Abbreviations

CFPB	Consumer Financial Protection Bureau
CIO	Chief Information Officer
DHS	U.S. Department of Homeland Security
FISMA	Federal Information Security Management Act of 2002
IG	Inspector General
ISCM	information security continuous monitoring
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SP 800-50	Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
SP 800-61	Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*
SP 800-128	Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
SP 800-137	Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
Treasury	U.S. Department of the Treasury

Executive Summary:

2013 Audit of the CFPB's Information Security Program

2013-IT-C-020 **December 2, 2013**

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). Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the CFPB's security controls and techniques as well as compliance by the CFPB with FISMA and related information security policies, procedures, standards, and guidelines.

Background

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program. FISMA also requires each agency Inspector General (IG) to conduct an annual independent evaluation of its agency's information security program and practices. The U.S. Department of Homeland Security (DHS) has issued guidance to IGs on FISMA reporting for 2013. This guidance directs IGs to evaluate the performance of agencies' information security programs across 11 areas.

Findings

Overall, we found that the CFPB has taken multiple steps over the past year to develop, document, and implement an information security program that is consistent with FISMA requirements. The CFPB has also taken several actions to strengthen its information security program in the 11 areas outlined in DHS's 2013 FISMA reporting guidance for IGs. We found that the CFPB's information security program is generally consistent with the requirements outlined in DHS's FISMA reporting guidance for IGs in 6 out of 11 information security areas: identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access management, and contractor systems.

We identified opportunities to improve CFPB's information security program through automation, centralization, and other enhancements to ensure that key DHS requirements for continuous monitoring, configuration management, and security training are met. Further, while we found CFPB's information security program to be generally consistent with DHS's requirements for incident response and reporting, we identified opportunities to strengthen CFPB's incident correlation processes.

We also identified improvements needed in contingency planning for a select system we reviewed. Our findings and recommendations for this system will be communicated under separate, restricted cover. Finally, we noted that the CFPB is taking sufficient actions to establish a security capital planning program, in accordance with the requirements outlined in DHS's FISMA reporting guidance for IGs. We will continue to monitor CFPB's efforts to improve its security capital planning program as part of our future FISMA audits.

Recommendations

Our report includes four recommendations designed to assist the CFPB in strengthening its information security program in the areas of continuous monitoring, configuration management, security training, and incident response and reporting. In a response to a draft of our report, the CFPB's Chief Information Officer concurred with our recommendations and outlined actions that have been taken, are underway, and are planned to strengthen CFPB's information security program.

Access the full report: http://www.consumerfinance.gov/oig/files/CFPB_Audit_Information_Security_FISMA_Dec2013.pdf

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

Summary of Recommendations, OIG Report No. 2013-IT-C-020

Rec. no.	Report page no.	Recommendation	Responsible office
1	5	Strengthen the CFPB's information security continuous monitoring program by a. defining and implementing performance measures to facilitate decisionmaking and improve performance of the agency's continuous monitoring program. b. identifying additional automated tools to assess security controls and analyze and respond to the results of continuous monitoring activities.	Office of the Chief Information Officer
2	7	Develop and implement an organization-wide configuration management plan and a consistent process for patch management.	Office of the Chief Information Officer
3	8	Design, develop, and implement a role-based security training program for individuals with significant security responsibilities.	Office of the Chief Information Officer
4	10	Ensure that audit logs and security incident information from all relevant sources are centrally tracked, analyzed, and correlated.	Office of the Chief Information Officer

OFFICE OF INSPECTOR GENERAL

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

December 2, 2013

MEMORANDUM

TO: Ashwin Vasan
Chief Information Officer, Consumer Financial Protection Bureau

FROM: Andrew Patchan Jr. Andrew Patchan Jr.
Associate Inspector General for Information Technology

SUBJECT: OIG Report No. 2013-IT-C-020: *2013 Audit of the CFPB's Information Security Program*

The Office of Inspector General is pleased to present its report on the 2013 audit of the information security program of the Consumer Financial Protection Bureau (CFPB). We performed this audit pursuant to requirements in the Federal Information Security Management Act of 2002, title III, Public Law 107-347 (December 17, 2002), which requires each agency Inspector General to conduct an annual independent evaluation of the agency's information security program and practices.

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 are planned to strengthen CFPB's information security program. As part of the 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 U.S. Department of Homeland Security's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*.

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

Attachment
cc: Sartaj Alag, Chief Operating Officer, CFPB
Matt Burton, Deputy Chief Information Officer, CFPB
Zachary Brown, Chief Information Security Officer, CFPB
Marla A. Freedman, Assistant Inspector General for Audit, Office of Inspector General,
U.S. Department of the Treasury
Mark Bialek, Inspector General
J. Anthony Ogden, Deputy Inspector General

Contents

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 as well as compliance by the CFPB with FISMA and related information security policies, procedures, standards, and guidelines. Our scope and methodology are detailed in appendix B.

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 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. FISMA also requires each agency Inspector General (IG) to perform an annual independent evaluation of the information security program and practices of its respective agency.

In support of FISMA's independent evaluation requirements, the U.S. Department of Homeland Security (DHS) has issued guidance to IGs on FISMA reporting for 2013.[2] This guidance directs IGs to evaluate the performance of agency information security programs across a variety of attributes grouped into 11 areas. These areas are continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, and security capital planning.

As noted in our 2012 FISMA audit report, when the CFPB began operations in July 2011, it relied on the information security program and systems of the U.S. Department of the Treasury (Treasury). The CFPB continues to rely on Treasury for certain information security program services and systems, including in the areas of remote access, security awareness training, and incident reporting. Our 2012 report also included three recommendations to assist the CFPB in developing, documenting, and implementing its own information security program. Specifically, we recommended that the CFPB's Chief Information Officer (CIO) finalize agency-wide information security policies and procedures, develop and implement a comprehensive information security strategy, and strengthen contractor oversight processes for

[1] Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (2002) (codified at 44 U.S.C. §§ 3541-3549).

[2] Department of Homeland Security, *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, November 30, 2012.

information security controls. Since 2012, the CFPB has made significant progress in developing, documenting, and implementing its information security program; as such, we are closing out our three FISMA audit recommendations from 2012.

Summary of Findings

Overall, we found that the CFPB has taken multiple steps over the past year to develop, document, and implement an information security program that is consistent with FISMA requirements. The CFPB has also taken several actions to strengthen its information security program in the 11 areas outlined in DHS’s 2013 FISMA reporting guidance for IGs. We found that the CFPB’s information security program is generally consistent with the requirements outlined in DHS’s FISMA reporting guidance for IGs in 6 out of 11 information security areas: identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access management, and contractor systems.

We identified opportunities to improve CFPB’s information security program through automation, centralization, and other enhancements to ensure that key DHS requirements for continuous monitoring, configuration management, and security training are met. Further, while we found CFPB’s information security program to be generally consistent with DHS’s requirements for incident response and reporting, we identified opportunities to strengthen CFPB’s incident correlation processes. For these improvement areas, we outline below the specific FISMA requirements, CFPB’s progress to date in meeting the requirements, work to be done, and provide a corresponding recommendation.

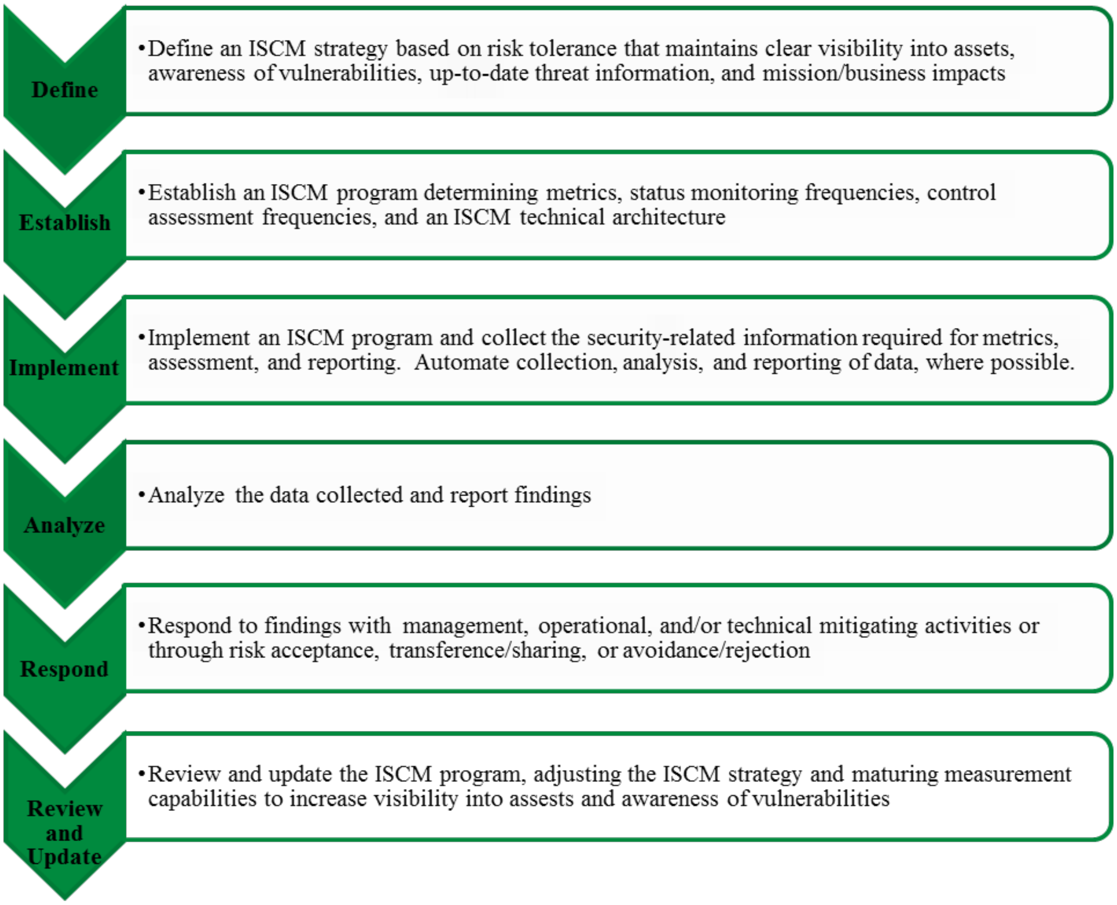
We also identified improvements needed in contingency planning for a select system we reviewed. Our findings and recommendations for this system will be communicated under separate, restricted cover. Finally, we noted that the CFPB is taking sufficient actions to establish a security capital planning program, in accordance with the requirements outlined in DHS’s FISMA reporting guidance for IGs. We will continue to monitor CFPB’s efforts to improve its security capital planning program as part of our future FISMA audits.

Continuous Monitoring

Requirement

FISMA requires agencies to perform periodic testing and evaluation of the effectiveness of their information security policies, procedures, and practices. To implement this requirement, guidance issued by the National Institute of Standards and Technology (NIST) and the DHS focuses on the process of information security continuous monitoring (ISCM). Specifically, ISCM is the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk-management decisions. The key components of an ISCM program are outlined in NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (SP 800-137) and highlighted in figure 1.

Figure 1: Components of an ISCM Program



Define
- Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts

Establish
- Establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture

Implement
- Implement an ISCM program and collect the security-related information required for metrics, assessment, and reporting. Automate collection, analysis, and reporting of data, where possible.

Analyze
- Analyze the data collected and report findings

Respond
- Respond to findings with management, operational, and/or technical mitigating activities or through risk acceptance, transference/sharing, or avoidance/rejection

Review and Update
- Review and update the ISCM program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assests and awareness of vulnerabilities

Source: Office of Inspector General analysis of NIST SP 800-137.

Progress to Date

The CFPB has taken several steps to develop and implement an ISCM program that is consistent with SP 800-137. For instance, the CFPB has developed policies, procedures, and an overall strategy for continuous monitoring. The CFPB's continuous monitoring strategy defines a process for ongoing security controls assessment, including identifying the security controls to be tested and the interval for assessment. The strategy also highlights the importance of vulnerability scanning in ensuring the protection of CFPB systems and data, and outlines frequencies for infrastructure, operating system, database, and application-level vulnerability scanning. In support of the continuous monitoring strategy, the CFPB has implemented change control processes and tools to track and analyze the security impact of changes. The CFPB is also utilizing an automated tool to perform weekly vulnerability scanning of the agency's operating systems and network devices.

Work to Be Done

We found that additional actions are needed to fully establish and implement CFPB's continuous monitoring strategy. Specifically, the CFPB has not defined metrics to facilitate decisionmaking and improve performance of its ISCM. NIST guidance notes that metrics can increase accountability, improve effectiveness of information security activities, and provide information for resource allocation decisions. We also noted opportunities to strengthen the CFPB's ISCM program through use of additional automated tools to more comprehensively assess security controls and system configurations. For instance, while the CFPB utilizes an automated tool to perform vulnerability assessments at the operating system and network levels, it does not have such tools to assess database and application-level vulnerabilities.

The CFPB finalized its continuous monitoring strategy in July 2013, and CFPB officials informed us that full implementation of the strategy is not expected until April 2014. Performance measures and automated tools to comprehensively assess security controls and system configurations will help the CFPB effectively identify information security weaknesses and manage all risks facing the organization.

Recommendation

We recommend that the CIO

1. Strengthen the CFPB's ISCM program by

    a. defining and implementing performance measures to facilitate decisionmaking and improve performance of the agency's continuous monitoring program.
    b. identifying additional automated tools to assess security controls and analyze and respond to the results of continuous monitoring activities.

Management's Response

The CIO concurred with our recommendation and noted that the CFPB is pursuing the use of additional automated tools and an improved use of performance measures to enhance its continuous monitoring program.

OIG Comment

In our opinion, the actions described by the CIO are responsive to our recommendation. We plan to follow up on the actions to ensure that the recommendation is fully addressed.

Configuration Management

Requirement

Configuration management refers to a collection of activities focused on establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring their configurations. From an information security perspective, configuration management refers to the management and control of secure configurations for an information system in accordance with organizational security requirements. FISMA requires agencies to develop and ensure compliance with minimally acceptable security configurations. Best practices for security-focused configuration management programs are outlined in NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (SP 800-128). SP 800-128 notes that federal agencies should develop and implement common, secure configuration settings for information systems and a robust patch management process to reduce vulnerabilities. SP 800-128 further states that agencies should develop a configuration management plan to describe how these processes will be managed across the organization.

Progress to Date

The CFPB has implemented components of an overall configuration management program. For instance, the CFPB has developed secure configuration settings and multiple security engineering baselines for technologies utilized at the agency. The CFPB has also implemented processes and an automated tool to manage information system changes and ensure that security impacts to configuration baselines are assessed and approved.

Work to Be Done

We found that the CFPB has not developed and implemented an organization-wide configuration management plan and a consistent process for patch management. A configuration management plan would provide a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of information systems. CFPB officials notified us that such a plan had not been developed, because the agency was focused on achieving operational capabilities and establishing its information technology infrastructure, as it transitioned away from Treasury. In a 2013 security control review of a CFPB system, we found that security patches for this system had not been installed in a timely manner and system devices were not securely configured in accordance with the CFPB's baseline configurations. An organization-wide configuration management plan can help ensure that CFPB systems are patched in a timely manner and securely configured.

Recommendation

We recommend that the CIO

2. Develop and implement an organization-wide configuration management plan and a consistent process for patch management.

Management's Response

The CIO concurred with our recommendation and noted that configuration management is a priority area for maturing CFPB's enterprise architecture in the coming year. In addition, the CIO noted that the CFPB plans to centralize the implementation of patch management.

OIG Comment

In our opinion, the actions described by the CIO are responsive to our recommendation. We plan to follow up on the actions to ensure that the recommendation is fully addressed.

Security Training

Requirement

FISMA requires agencies to provide security awareness training to all information system users to inform them of risks associated with their activities and their responsibilities in complying with security policies and procedures. FISMA also requires agencies to provide role-based training to individuals with significant security responsibilities. The primary difference between security awareness training and role-based training is that the former is geared toward focusing all users on overall information security policies, while the latter is geared toward teaching information security skills needed to perform specific information technology functions. Best practices for developing and implementing a security training program are outlined in NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program* (SP 800-50). SP 800-50 highlights the important role that training plays in ensuring the effective implementation of an agency's information security program and notes that individuals with significant security responsibilities include system and network administrators, managers, and security officers. SP 800-50 also identifies four critical steps in the life cycle of an information technology security awareness and training program. These steps are program design, development, implementation, and post-implementation.

Progress to Date

The CFPB has developed and implemented security awareness training that is required to be completed by all employees and contractors on an annual basis. Our review of the content of the CFPB's security awareness training found that it included topics recommended in SP 800-50 and other best practices. In addition, the CFPB conducts information security awareness training sessions every two weeks, provides security awareness training in new hire briefings, and provides ongoing security awareness updates on the agency's intranet site and other internal mediums.

Work to Be Done

The CFPB has not designed, developed, and implemented a role-based training program for individuals with significant security responsibilities. We attribute this to the recent finalization of key CFPB policies and procedures that outline roles and responsibilities for individuals with significant security responsibilities. Further, in 2013, the CFPB focused on transitioning security awareness services from Treasury before establishing a role-based security training program. A role-based security training program will help provide the CFPB with assurance that employees and contractor staff with significant security responsibilities have adequate knowledge and expertise to ensure the effective and efficient implementation of the agency's information security program.

Recommendation

We recommend that the CIO

3. Design, develop, and implement a role-based security training program for individuals with significant security responsibilities.

Management's Response

> The CIO concurred with our recommendation and noted that the CFPB plans to finalize its current role-based security training strategy and ensure that individuals with significant security responsibilities receive appropriate training.

OIG Comment

> In our opinion, the actions described by the CIO are responsive to our recommendation. We plan to follow up on the actions to ensure that the recommendation is fully addressed.

Incident Response and Reporting

Requirement

FISMA requires agencies to develop and implement procedures for detecting, reporting, and responding to security incidents, including mitigating risks of such incidents before substantial damage is done. Best practices for establishing incident detection, reporting, and response capabilities are outlined in NIST Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide* (SP 800-61). SP 800-61 states that agencies should create an incident response policy, plan, and procedures. Further, given the multitude of sources and signs of incident activity occurring in organizations' information systems, SP 800-61 emphasizes the importance of using automated correlation and centralized logging tools to analyze incident data. Correlating events among multiple indicator sources can be valuable in detecting whether a particular incident occurred as well as in mitigating risks before substantial damage is done.

Progress to Date

The CFPB has taken several steps to develop a capability to detect, report, and respond to security incidents. For example, the CFPB has developed an organization-wide incident response policy and plan that defines the processes and roles and responsibilities for computer incident response activities at the CFPB, including for third-party providers. The CFPB has also established a computer security incident response team and developed a centralized tracking tool for documenting, monitoring, and ensuring adequate response to incidents. Further, the CFPB is in the process of building a tool to collect audit logging and incident data from various systems to support the detection, validation, and correlation of incidents.

Work to Be Done

We found that the CFPB had not fully implemented a capability to correlate information on incident activity. Specifically, the tool used by the CFPB to collect audit logging and incident data across CFPB systems does not yet include data from all relevant sources, including some third-party systems. For a select system that we reviewed, we noted that while a variety of audit and incident logs were being generated by system devices, they were not being centrally analyzed or correlated for anomalous activity. Weaknesses in CFPB's capability to comprehensively correlate events among multiple indicator sources are a result of the developing maturity of the CFPB's incident management program. Specifically, agency officials have prioritized establishing the policies, procedures, and overall structure of the CFPB's incident response capability. Centrally analyzed and correlated information on incident activity will help ensure that the CFPB can fully detect and respond to information security incidents in a timely manner.

Recommendation

We recommend that the CIO

4. Ensure that audit logs and security incident information from all relevant sources are centrally tracked, analyzed, and correlated.

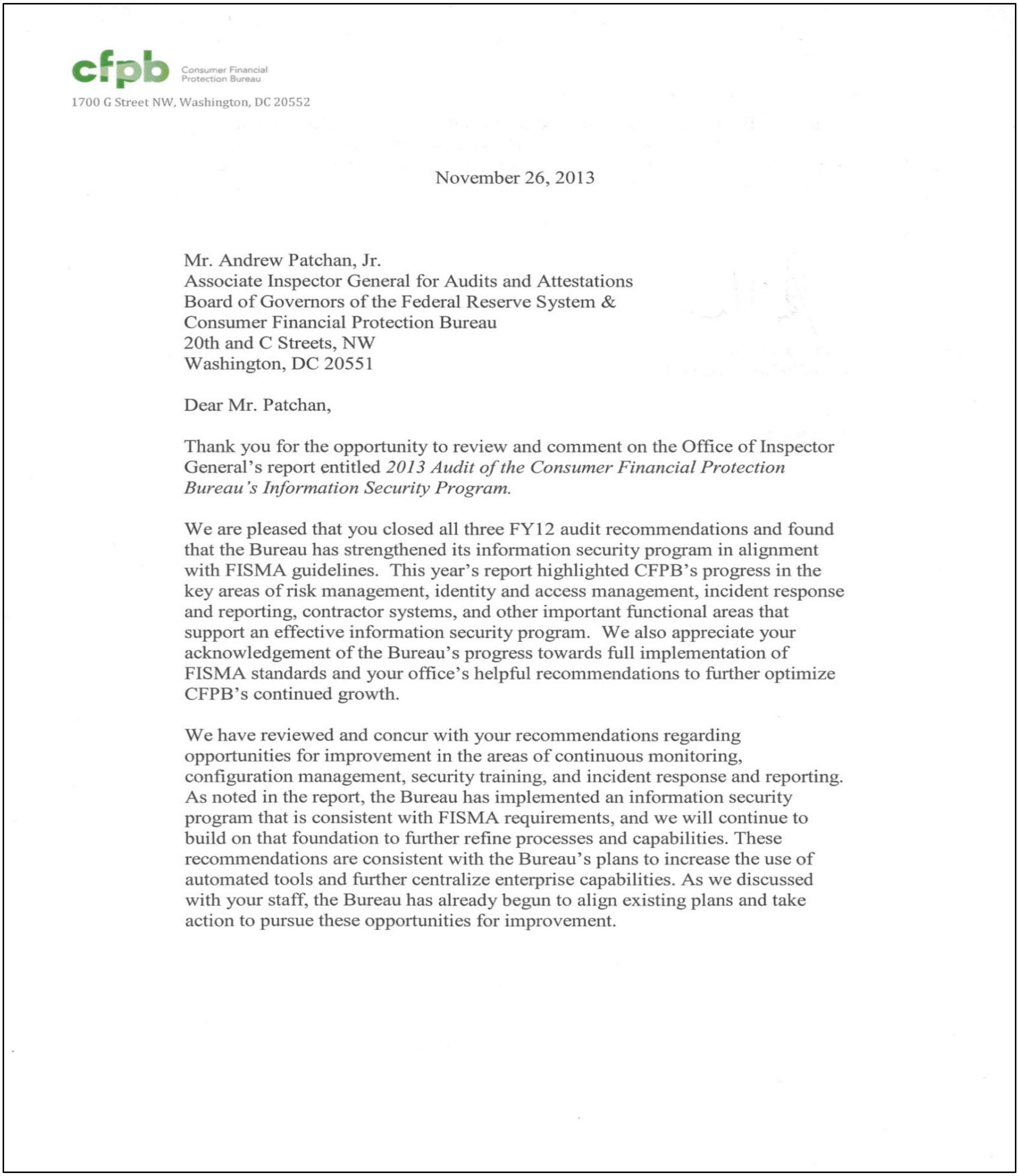
Management's Response

The CIO concurred with our recommendation and noted that the CFPB plans to further automate the collection, correlation, and reporting of audit logs and security incident information in fiscal year 2014.

OIG Comment

In our opinion, the actions described by the CIO are responsive to our recommendation, and we plan to follow up on the actions to ensure that the recommendation is fully addressed.

Appendix A
Management's Response



cfpb Consumer Financial Protection Bureau

1700 G Street NW, Washington, DC 20552

November 26, 2013

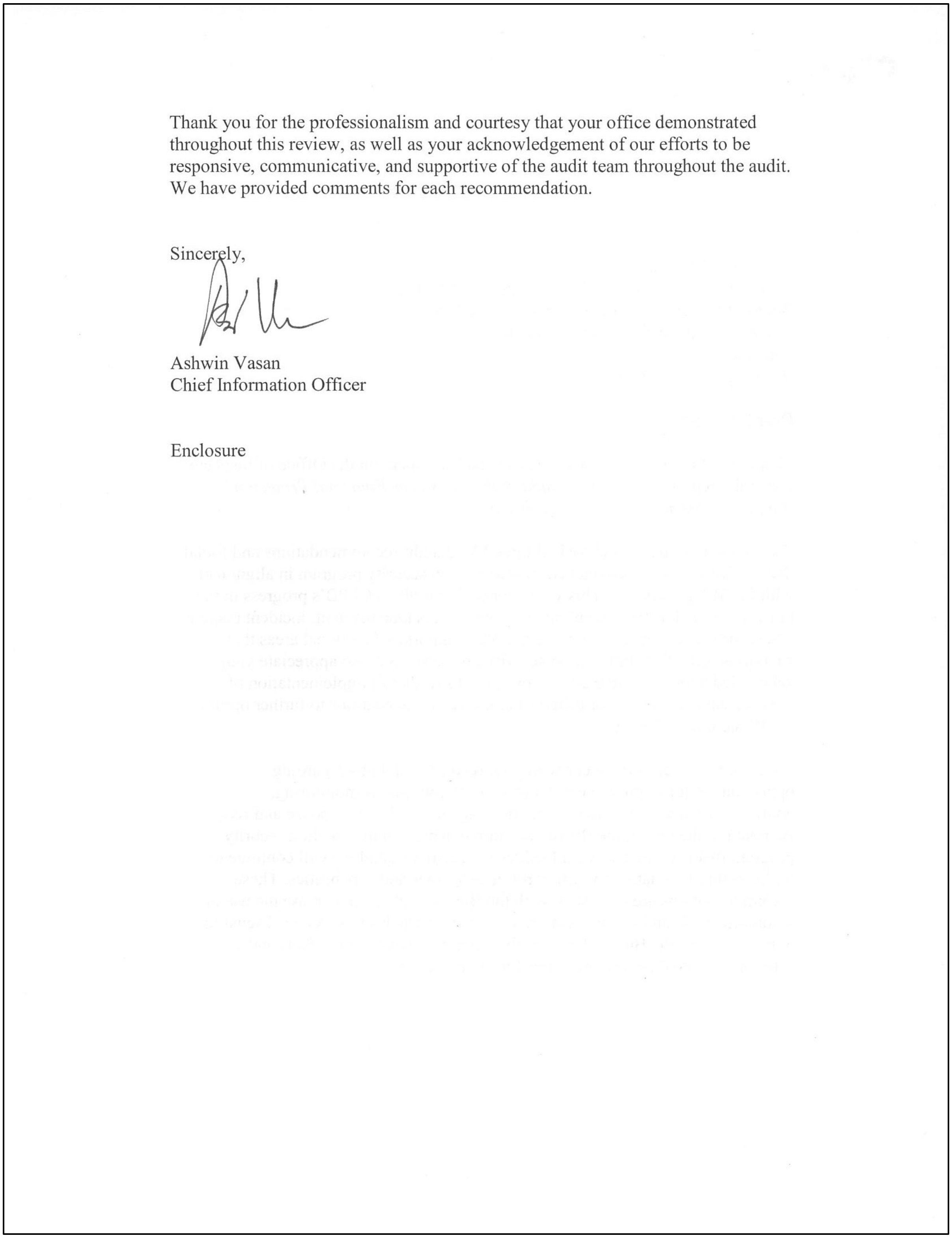
Mr. Andrew Patchan, Jr.
Associate Inspector General for Audits and Attestations
Board of Governors of the Federal Reserve System &
Consumer Financial Protection Bureau
20th and C Streets, NW
Washington, DC 20551

Dear Mr. Patchan,

Thank you for the opportunity to review and comment on the Office of Inspector General's report entitled *2013 Audit of the Consumer Financial Protection Bureau's Information Security Program.*

We are pleased that you closed all three FY12 audit recommendations and found that the Bureau has strengthened its information security program in alignment with FISMA guidelines. This year's report highlighted CFPB's progress in the key areas of risk management, identity and access management, incident response and reporting, contractor systems, and other important functional areas that support an effective information security program. We also appreciate your acknowledgement of the Bureau's progress towards full implementation of FISMA standards and your office's helpful recommendations to further optimize CFPB's continued growth.

We have reviewed and concur with your recommendations regarding opportunities for improvement in the areas of continuous monitoring, configuration management, security training, and incident response and reporting. As noted in the report, the Bureau has implemented an information security program that is consistent with FISMA requirements, and we will continue to build on that foundation to further refine processes and capabilities. These recommendations are consistent with the Bureau's plans to increase the use of automated tools and further centralize enterprise capabilities. As we discussed with your staff, the Bureau has already begun to align existing plans and take action to pursue these opportunities for improvement.

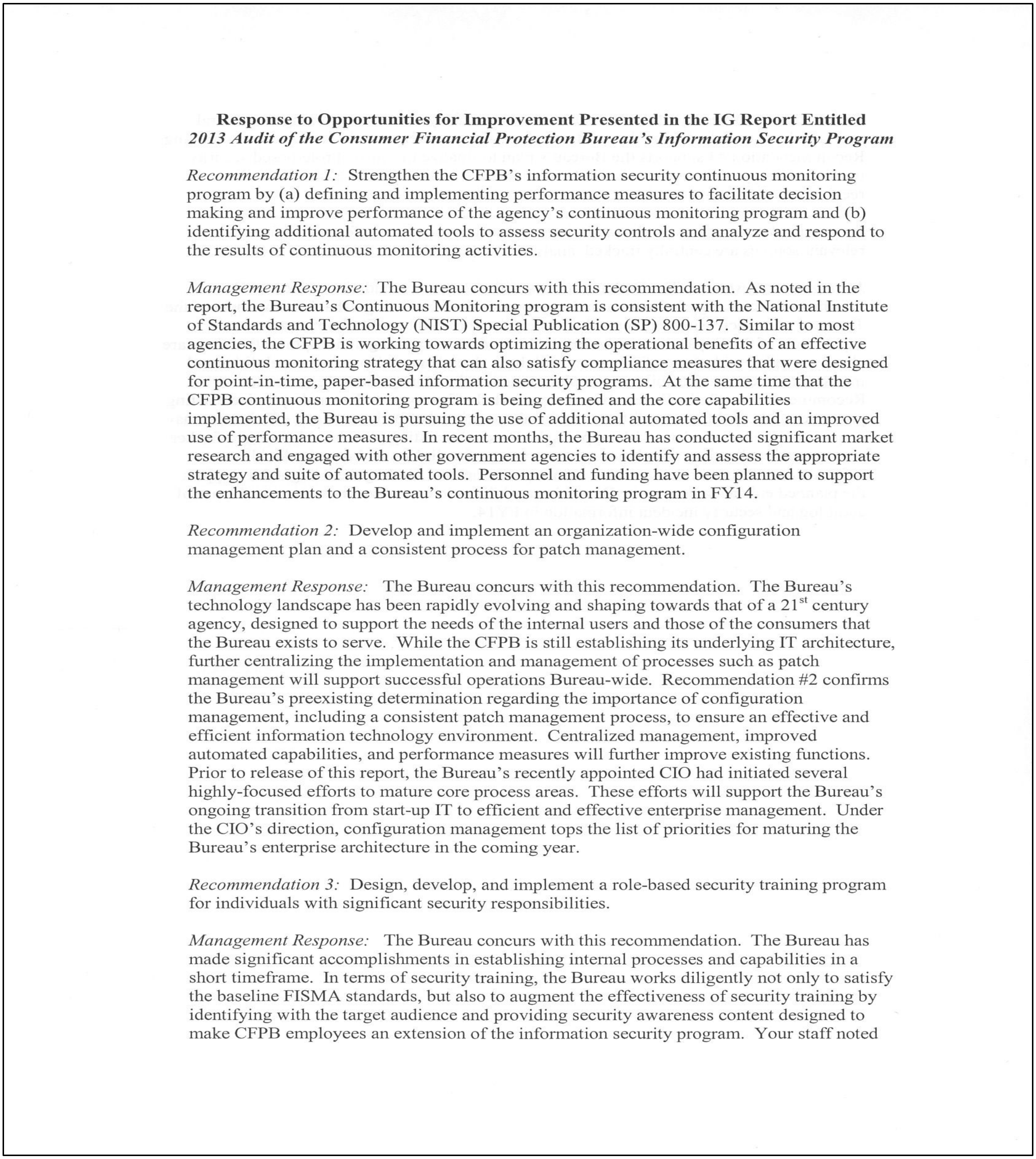


Thank you for the professionalism and courtesy that your office demonstrated throughout this review, as well as your acknowledgement of our efforts to be responsive, communicative, and supportive of the audit team throughout the audit. We have provided comments for each recommendation.

Sincerely,

Ashwin Vasan
Chief Information Officer

Enclosure



Response to Opportunities for Improvement Presented in the IG Report Entitled
2013 Audit of the Consumer Financial Protection Bureau's Information Security Program

Recommendation 1: Strengthen the CFPB's information security continuous monitoring program by (a) defining and implementing performance measures to facilitate decision making and improve performance of the agency's continuous monitoring program and (b) identifying additional automated tools to assess security controls and analyze and respond to the results of continuous monitoring activities.

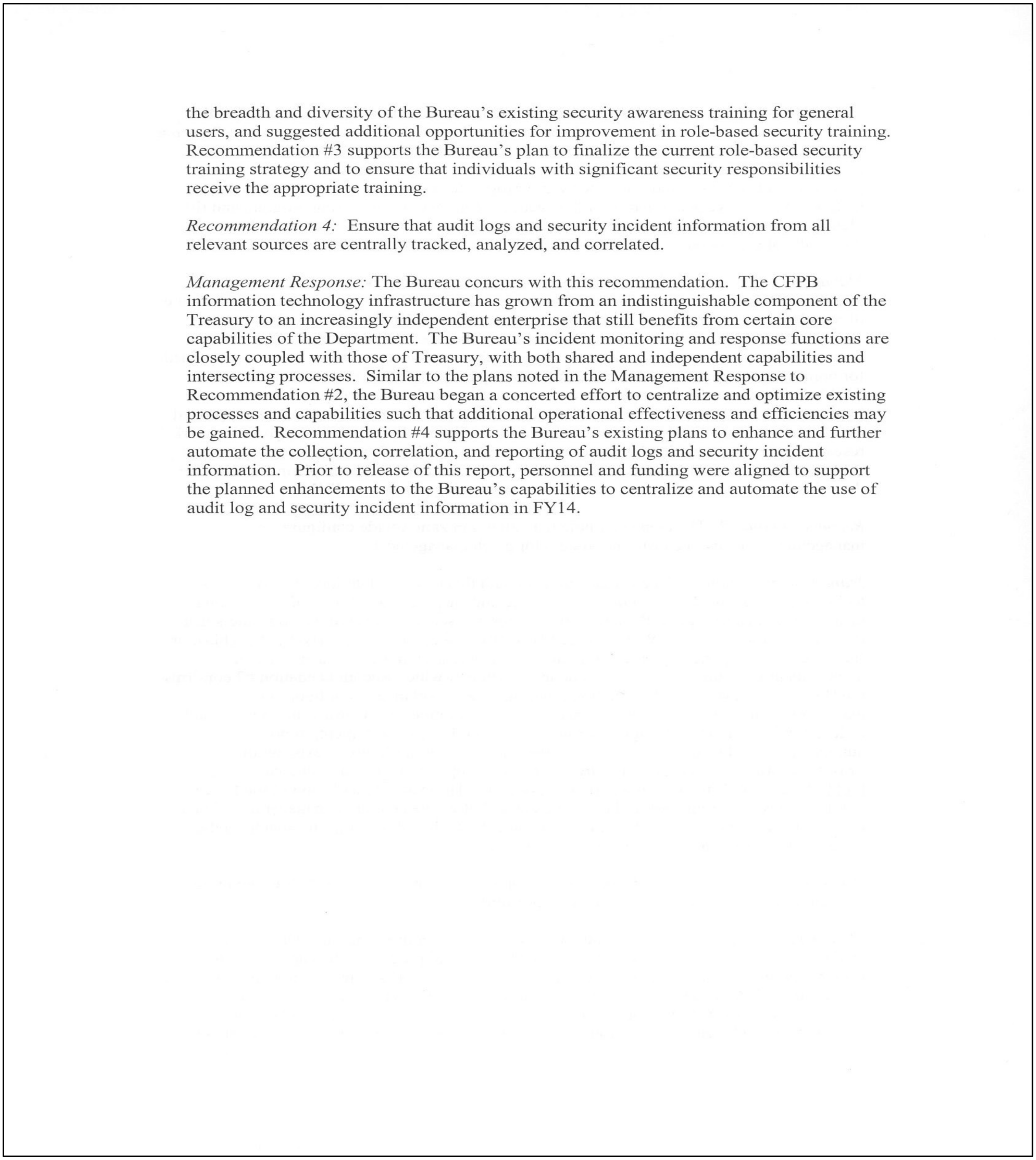
Management Response: The Bureau concurs with this recommendation. As noted in the report, the Bureau's Continuous Monitoring program is consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137. Similar to most agencies, the CFPB is working towards optimizing the operational benefits of an effective continuous monitoring strategy that can also satisfy compliance measures that were designed for point-in-time, paper-based information security programs. At the same time that the CFPB continuous monitoring program is being defined and the core capabilities implemented, the Bureau is pursuing the use of additional automated tools and an improved use of performance measures. In recent months, the Bureau has conducted significant market research and engaged with other government agencies to identify and assess the appropriate strategy and suite of automated tools. Personnel and funding have been planned to support the enhancements to the Bureau's continuous monitoring program in FY14.

Recommendation 2: Develop and implement an organization-wide configuration management plan and a consistent process for patch management.

Management Response: The Bureau concurs with this recommendation. The Bureau's technology landscape has been rapidly evolving and shaping towards that of a 21st century agency, designed to support the needs of the internal users and those of the consumers that the Bureau exists to serve. While the CFPB is still establishing its underlying IT architecture, further centralizing the implementation and management of processes such as patch management will support successful operations Bureau-wide. Recommendation #2 confirms the Bureau's preexisting determination regarding the importance of configuration management, including a consistent patch management process, to ensure an effective and efficient information technology environment. Centralized management, improved automated capabilities, and performance measures will further improve existing functions. Prior to release of this report, the Bureau's recently appointed CIO had initiated several highly-focused efforts to mature core process areas. These efforts will support the Bureau's ongoing transition from start-up IT to efficient and effective enterprise management. Under the CIO's direction, configuration management tops the list of priorities for maturing the Bureau's enterprise architecture in the coming year.

Recommendation 3: Design, develop, and implement a role-based security training program for individuals with significant security responsibilities.

Management Response: The Bureau concurs with this recommendation. The Bureau has made significant accomplishments in establishing internal processes and capabilities in a short timeframe. In terms of security training, the Bureau works diligently not only to satisfy the baseline FISMA standards, but also to augment the effectiveness of security training by identifying with the target audience and providing security awareness content designed to make CFPB employees an extension of the information security program. Your staff noted



the breadth and diversity of the Bureau's existing security awareness training for general users, and suggested additional opportunities for improvement in role-based security training. Recommendation #3 supports the Bureau's plan to finalize the current role-based security training strategy and to ensure that individuals with significant security responsibilities receive the appropriate training.

Recommendation 4: Ensure that audit logs and security incident information from all relevant sources are centrally tracked, analyzed, and correlated.

Management Response: The Bureau concurs with this recommendation. The CFPB information technology infrastructure has grown from an indistinguishable component of the Treasury to an increasingly independent enterprise that still benefits from certain core capabilities of the Department. The Bureau's incident monitoring and response functions are closely coupled with those of Treasury, with both shared and independent capabilities and intersecting processes. Similar to the plans noted in the Management Response to Recommendation #2, the Bureau began a concerted effort to centralize and optimize existing processes and capabilities such that additional operational effectiveness and efficiencies may be gained. Recommendation #4 supports the Bureau's existing plans to enhance and further automate the collection, correlation, and reporting of audit logs and security incident information. Prior to release of this report, personnel and funding were aligned to support the planned enhancements to the Bureau's capabilities to centralize and automate the use of audit log and security incident information in FY14.

Appendix B
Objective, Scope, and Methodology

Our specific audit objectives were to evaluate the effectiveness of the CFPB's security controls and techniques as well as compliance by the CFPB with FISMA and related information security policies, procedures, standards, and guidelines. To accomplish our objectives, we reviewed the effectiveness of the CFPB's information security program across the 11 areas outlined in DHS's 2013 FISMA reporting guidance for IGs. These areas include continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, and security capital planning. To assess the CFPB's information security program in these areas, we interviewed CFPB management, staff, and contractors; analyzed security policies, procedures, and documentation; and observed and tested specific security processes and controls. We also assessed the implementation of select security controls for a contractor-operated system listed on the CFPB's FISMA inventory and performed vulnerability scanning on select system devices.

We utilized the results of our review of the CFPB's information security program and testing of controls for a select system to evaluate the implementation of specific attributes outlined in DHS's 2013 FISMA reporting guidance for IGs. As noted in our report, the CFPB is relying on Treasury for specific information security program services. These services include remote access and identity and access management. To evaluate specific attributes outlined in DHS's FISMA reporting guidance for remote access and identity and access management, we relied on the work performed by the Treasury Office of Inspector General (OIG) as part of its 2013 FISMA review of Treasury's information security program. We performed sufficient, appropriate procedures to meet requirements outlined in generally accepted government auditing standards for relying on the work of other audit organizations, including the following:

- We obtained evidence of the qualifications and independence of contractor staff performing the FISMA audit of Treasury for the Treasury OIG.
- We reviewed the Treasury OIG's FISMA audit plan, audit report, work paper documentation, and latest peer review report.
- 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 conducted our fieldwork from June 2013 to September 2013. 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.

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