OFFICE OF INSPECTOR GENERAL

Audit Report 2014-IT-C-020

2014 Audit of the CFPB's Information Security Program

November 14, 2014

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

Report Contributors

Khalid Hasan, OIG Manager
Joshua Dieckert, Auditor-in-Charge
Daniel Megalo, 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
ConOps	*United States Government Concept of Operations for Information Security Continuous Monitoring*
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 2, *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:

2014 Audit of the CFPB's Information Security Program

2014-IT-C-020 November 14, 2014

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 the agency's information security program, practices, and controls for select systems. The U.S. Department of Homeland Security (DHS) has issued guidance to IGs on FISMA reporting for 2014. This guidance directs IGs to evaluate the performance of agencies' information security programs across 11 areas.

Findings

The CFPB continues to take steps to mature its information security program and ensure that it is consistent with the requirements of FISMA. Overall, we found that the CFPB's information security program is consistent with the requirements outlined in DHS's FISMA reporting guidance for IGs in 9 out of 11 areas: information security continuous monitoring (ISCM), configuration management, identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access, contractor systems, and security capital planning. Although corrective actions are underway, further improvements are needed in security training and contingency planning.

While we found that the CFPB's information security program was generally consistent with the requirements for ISCM, configuration management, and incident response, we identified opportunities to strengthen these areas through automation and centralization. This year, we found that the Chief Information Officer (CIO) has taken actions to address our 2013 recommendation related to ISCM; however, the CFPB's ISCM program continues to depend on manual, labor-intensive processes. As such, we are closing our 2013 recommendation for ISCM and issuing two additional recommendations to further strengthen the CFPB's ISCM program. In addition, our 2013 FISMA audit report included recommendations to develop and implement (1) an organization-wide configuration management plan and consistent process for patch management, (2) a capability to centrally track and analyze audit logs and security incident information, and (3) a role-based training program. Corrective actions to address these recommendations have not been finalized. As such, we are leaving these recommendations open and will continue to monitor the CFPB's progress in these areas as part of future FISMA audits. We also have a new recommendation for improving configuration management.

Recommendations

Our report includes three new recommendations designed to strengthen the CFPB's ISCM and configuration management practices. We recommend that the CIO (1) fully implement the CFPB's selected automated solution for assessing security controls and analyzing and responding to the results of continuous monitoring activities, and (2) assess the ISCM implementation options and guidance outlined in the *United States Government Concept of Operations for Information Security Continuous Monitoring* and update the CFPB's ISCM strategy, as necessary. We also recommend that the CIO strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.

In response to our report, the CIO concurred with our recommendations and outlined actions that have been taken, are underway, and are planned to strengthen the CFPB's information security program.

Summary of Recommendations, OIG Report No. 2014-IT-C-020

Rec. no.	Report page no.	Recommendation	Responsible office
1	4	Fully implement the CFPB's selected automated solution for assessing security controls and analyzing and responding to the results of continuous monitoring activities.	Office of the Chief Information Officer
2	4	Assess the information security continuous monitoring implementation options and guidance outlined in the *United States Government Concept of Operations for Information Security Continuous Monitoring* and update the CFPB's information security continuous monitoring strategy, as necessary.	Office of the Chief Information Officer
3	6	Strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.	Office of the Chief Information Officer

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

November 14, 2014

MEMORANDUM

TO: Ashwin Vasan
Chief Information Officer
Consumer Financial Protection Bureau

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

SUBJECT: OIG Report No. 2014-IT-C-020: *2014 Audit of the CFPB's Information Security Program*

The Office of Inspector General is pleased to present its report on the 2014 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.

As part of the audit, we also reviewed security controls for two select agency systems. The detailed results of our reviews of the security controls for these systems will be transmitted under separate, restricted cover. In addition, we will use 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 2014 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.

cc: Sartaj Alag, Chief Operating Officer, CFPB
Stephen Agostini, Chief Financial 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
J. Anthony Ogden, Deputy Inspector General
Matthew Simber, OIG Manager for Policy, Planning, and Quality Assurance

Contents

Introduction

Objectives

Our specific audit objectives, based on the requirements of the Federal Information Security Management Act of 2002 (FISMA), were to evaluate the effectiveness of the Consumer Financial Protection Bureau's (CFPB) 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 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 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, including testing controls for select systems.

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 2014.[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 2013 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). While the CFPB's information security program is now operating largely independent of Treasury, the agencies continue to share operational responsibilities for several security functions, including information security continuous monitoring (ISCM), remote access, security awareness and training, and incident reporting. CFPB officials informed us that as the agency transitions away from Treasury's wide area network and infrastructure by the end of 2014, these security functions will be performed solely by the CFPB.

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. U.S. Department of Homeland Security, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, December 2, 2013.

Summary of Findings

The CFPB continues to take steps to mature its agency-wide information security program. For instance, we found that the Chief Information Officer (CIO) has implemented ongoing security controls testing for the CFPB's systems and improved patch management practices. We found that the CFPB's information security program is generally consistent with attributes identified in DHS's FISMA reporting guidance for IGs in 9 out of 11 information security areas: continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access, contractor systems, and security capital planning. Although corrective actions are underway, further improvements are needed to implement the attributes outlined in DHS's FISMA reporting guidance for the remaining two information security areas: security training and contingency planning. The improvement opportunities related to contingency planning result from system testing that we performed to support our FISMA work, the results of which will be transmitted under separate, restricted cover.

While we found that the CFPB's information security program is generally consistent with the requirements for ISCM, configuration management, and incident response, we identified opportunities to strengthen these areas through automation and centralization. Specifically, in our 2013 FISMA audit report, we recommended that the CIO strengthen the CFPB's ISCM program by defining and implementing performance measures, and identifying additional automated tools to support ISCM processes. This year, we found that the CIO has taken actions to address our 2013 recommendation; however, the CFPB's ISCM program continues to depend on manual, labor-intensive processes. As such, we are closing our 2013 recommendation for ISCM and issuing two additional recommendations to further strengthen the CFPB's ISCM program through additional automation.

In addition, our 2013 FISMA audit report included recommendations to develop and implement (1) an organization-wide configuration management plan and consistent process for patch management, (2) a capability to centrally track and analyze audit logs and security incident information, and (3) a role-based training program. Corrective actions to address these recommendations have not been finalized. As such, we are leaving these recommendations open and will continue to monitor the CFPB's progress in these areas as part of future FISMA audits. This year, we also identified an additional opportunity to strengthen the CFPB's vulnerability management practices for database and application-level security configurations, and we are issuing a new recommendation in this area.

Analysis of the CFPB's Progress in Implementing Key FISMA and DHS Information Security Program Requirements

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 DHS focuses on the process of ISCM to support ongoing system authorization. Specifically, ISCM is defined as the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk-management decisions. NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (SP 800-137) notes that ISCM can be efficiently performed using both manual and automated processes. In particular, SP 800-137 emphasizes that automation can enable greater consistency and reliability of ISCM through ongoing security control assessments, reporting of security status, and the collection of security metrics across the organization.

To supplement NIST guidance on ISCM, the Federal CIO Council issued the *United States Government Concept of Operations for Information Security Continuous Monitoring* (ConOps) in October 2013. The ConOps provides a roadmap for the realization and operationalization of ISCM throughout the federal government using a three-phased approach to be implemented by fiscal year 2017. The phased approach includes performing ISCM for local computing devices (e.g., servers, clients, and the applications that run on them), the network and infrastructure (e.g., routers, switches), and the organization's enclave boundary (e.g., firewalls and remote access connections at the point at which information enters or leaves the organization's network).

The ConOps outlines three options for agencies to implement ISCM: (1) a "do-it-yourself" approach using commercial off-the-shelf or government off-the-shelf tools; (2) the DHS Continuous Diagnostics and Mitigation program; and (3) a hybrid approach combining the first two options. The ConOps notes that agencies should evaluate the pros and cons of each option and consider various criteria, including return on investment, privacy/security concerns, and flexibility, when selecting an implementation strategy.

Progress to Date

Our 2013 FISMA audit included a recommendation that the CIO strengthen the CFPB's ISCM program by (1) defining and implementing performance measures to facilitate decisionmaking and improve performance of the agency's continuous monitoring program and (2) identifying additional automated tools to assess security controls and analyze and respond to the results of continuous monitoring activities. In 2014, we found that the CIO has taken several steps to implement an ISCM program that is consistent with SP 800-137 and to respond to our recommendation. For instance, the CFPB is performing ongoing assessment

and reporting of security control status for the agency's systems. As part of this process, the agency is tracking performance measures related to the implementation status of security controls. In addition, the CIO has identified a number of tools to assess controls and analyze and respond to the results of continuous monitoring activities. As such, we are closing our continuous monitoring recommendation from last year.

Work to Be Done

The CIO has recently procured an automated solution to support ISCM activities and security control assessments; however, this tool has not yet been fully implemented across the CFPB. Currently, components of the CFPB's ISCM program rely on manual and labor-intensive processes. For instance, to complete ongoing control assessments, the CFPB's Cybersecurity Office must first individually reach out to system security officials across the agency to schedule testing activities based on the frequencies established in the agency's ISCM strategy. Security officials provide testing results in spreadsheets, which are then manually analyzed and compiled into a monthly report for review by senior management. Due to the manual nature of this process, the CFPB may not be able to provide timely reporting on control effectiveness to senior management. We believe that full implementation of the procured automated solution will provide the CIO with more comprehensive and timely information to make risk-based decisions.

We also found that the CFPB has not formally evaluated and selected how the agency plans to implement ISCM in accordance with the ConOps. One reason is that the CFPB is in the process of transitioning several information technology and telecommunications services from Treasury that will impact this decision. CFPB officials informed us that the agency plans to transition these activities from Treasury by the end of 2014. We believe that by evaluating the ISCM implementation options outlined in the ConOps, the agency will be better informed of the appropriate steps necessary to implement its ISCM strategy.

Recommendation

We recommend that the CIO

1. Fully implement the CFPB's selected automated solution for assessing security controls and analyzing and responding to the results of continuous monitoring activities.

2. Assess the ISCM implementation options and guidance outlined in the ConOps and update the CFPB's ISCM strategy, as necessary.

Management's Response

In response to recommendation 1, the CIO concurred with our recommendation and stated that the CFPB plans to continue to develop and improve its ISCM automated capabilities.

In response to recommendation 2, the CIO concurred with our recommendation and stated that the agency has taken action to align its ISCM implementation strategy with the ISCM options and guidance outlined in the ConOps.

OIG Comment

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

Configuration Management

Requirement

From an information security perspective, configuration management refers to establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring their security configurations. 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

Our 2013 FISMA audit included a recommendation that the CIO develop and implement an organization-wide configuration management plan and a consistent process for patch management. In 2014, we found that the CFPB continues to mature its configuration management program. For instance, the CIO finalized an organization-wide patch management policy to ensure that software patches are installed in a safe and timely manner. As we noted last year, the CIO has also implemented processes and automated tools to assess configuration settings, manage security baseline deviations, and ensure that security impacts to configuration changes are assessed and approved. In addition, as part of our vulnerability scanning of two select CFPB systems, we noted improvements in the implementation of the CFPB's security configuration settings and installation of patches at the operating system level.

Work to Be Done

As part of our follow-up work to our 2013 FISMA audit recommendations, we found that the CIO has not developed and implemented an organization-wide configuration management plan and fully implemented the recently issued patch management policy. Specifically, our 2014 security control reviews of two CFPB systems identified improvements needed in the patching and secure configuration of database and application servers. In addition, we identified application user and system accounts that were granted privileges beyond those that were

required. A contributing factor for these issues was that the CFPB has not yet implemented security tools to periodically check for database and application-level misconfigurations. Our specific recommendations for these two CFPB systems will be transmitted under separate, restricted cover.

As we noted in 2013, the full implementation of an organization-wide configuration management plan and consistent patch management process can help ensure that all components of CFPB systems are securely configured. We will leave this recommendation open and continue to follow up on the CIO's actions as part of our future FISMA audits. In addition, we believe that the implementation of additional automated tools and a process to periodically assess and manage database and application-level security misconfigurations can help ensure the confidentiality, integrity, and availability of CFPB systems.

Recommendation

We recommend that the CIO

3. Strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.

Management's Response

The CIO concurred with our recommendation and stated that plans to continue the evolution of vulnerability management in the enterprise are underway and are on track for further improvements in FY 2015.

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 2, *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

Our 2013 FISMA audit included a recommendation that the CIO ensure that audit logs and security incident information from all relevant sources are centrally tracked, analyzed, and correlated. This year, we found that the CFPB continues to take steps to strengthen its capability to detect, report, and respond to security incidents. For instance, the CIO is in the process of procuring an automated solution to perform centralized audit monitoring and incident correlation functions. In addition, CFPB officials informed us that the agency has established a security operations center, as well as relationships with federal incident coordination entities, as the agency prepares for the migration of its wide area network from Treasury.

Work to Be Done

As part of our follow-up work to our 2013 FISMA audit, we found that the CFPB has not yet developed a capability to correlate audit log and security incident information. As we noted last year, 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. We will leave our 2013 recommendation open in this area and continue to follow up on the CIO's actions as part of our future FISMA audits.

Security Training

Requirement

FISMA requires agencies to provide security awareness training to all information system users and role-based security 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, security program 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, material development, program implementation, and post-implementation.

Progress to Date

Our 2013 FISMA audit included a recommendation that the CIO design, develop, and implement a role-based security training program for individuals with significant information security responsibilities. We also noted that the CFPB had developed and implemented a security awareness training program that was consistent with SP 800-50 and other best practices. This year, we found that the CFPB continues to conduct 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. In addition, the CIO has taken several steps to design and develop a role-based security training program. For instance, the CIO has developed a draft policy detailing the individuals requiring role-based training, along with a specific curriculum for each role. The CFPB is also piloting an automated solution designed to offer and track role-based training for employees and contractors.

Work to Be Done

As part of our follow-up work to our 2013 FISMA audit, we found that the CIO has not yet fully implemented a role-based security training program. As we noted last year, 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. We will leave our 2013 recommendation regarding the implementation of a role-based security training program open and continue to follow up on the CIO's actions as part of our future FISMA audits.

Appendix A
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 2014 FISMA reporting guidance for IGs. 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. 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 two agency systems on the CFPB's FISMA inventory and performed vulnerability scanning at the operating system, network, and application levels on select system devices.

We utilized the results of our review of the CFPB's information security program and testing of controls for select systems to evaluate the implementation of specific attributes outlined in DHS's 2014 FISMA reporting guidance for IGs. As noted in our report, the CFPB's information security program is operating largely independently; however, the agency relies on Treasury for specific information security program services, including in the areas of remote access, security training, incident reporting, and identity and access management. To evaluate specific attributes outlined in DHS's FISMA reporting guidance for these areas, we relied on the work performed by the Treasury Office of Inspector General (OIG) as part of its 2014 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 evaluation of Treasury for the Treasury OIG.
- We reviewed the Treasury OIG's FISMA evaluation plan, final report, workpaper 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 their processes to review the work performed by contractor staff.

We performed our fieldwork from June 2014 to October 2014. 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.

cfpb Consumer Financial Protection Bureau
1700 G Street NW, Washington, DC 20552

November 13, 2014

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

Thank you for the opportunity to review and comment on the Office of Inspector General's draft report of the *2014 Audit of the CFPB's Information Security Program.*

We are pleased that you found that the Bureau continues to improve our FISMA compliance and Information Security posture. The report noted measures taken by the CFPB to implement ongoing security controls testing for CFPB's systems as part of our continuous monitoring process, and also noted that we have improved our patch management practices at the operating system level. During FY2014, the Bureau successfully executed the first full year of Information Security Continuous Monitoring (ISCM) activity, from which we have gleaned valuable insight from ISCM into the methods and metrics that support our continuous authorization model. Our current ISCM strategy and Continuous Diagnostics and Mitigation (CDM) plans coincide with your recommendations conveyed in this year's report and align to our plans and expectations for maturing the program. We appreciate that you have closed 2013's recommendation on continuous monitoring, and the Bureau looks forward to further noteworthy improvements in continuous monitoring in the year to come.

The Bureau is pleased to note that you now record us as consistent with nine of the eleven OIG FISMA areas, specifically continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access management, contractor systems, and security capital planning. We are glad that our efforts to enhance continuous monitoring, configuration management, and security capital planning are reflected in your report, significantly improving the results from last year. In FY2015, we will continue our work to incrementally improve and mature our processes in the areas of security training and contingency planning.

In your report, you noted our progress not only in ISCM, but also our work in configuration management (CM), the ongoing maturation of our CM program, and the progress we have made through the finalization of our organization-wide patch management policy. This policy is one element to our comprehensive plans to improve assurances that software patches are installed in a safe and timely manner, and that systems remain in a compliant, risk-tolerant state. Our existing plans, to improve overall vulnerability management through the use of more advanced CM and vulnerability management tools will result in improvements that address your recommendations in this year's report.

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

Sincerely,

ASHWIN VASAN

Digitally signed by ASHWIN VASAN
DN: c=US, o=U.S. Government, ou=Consumer Financial Protection Bureau, cn=ASHWIN VASAN, 0.9.2342.19200300.100.1.1=95581002465793
Date: 2014.11.14 10:05:15 -05'00'

Ashwin Vasan
Chief Information Officer

Response to Recommendations Presented in the Draft IG Report
2014 Audit of the CFPB's Information Security Program

Recommendation 1: Fully implement the CFPB's selected automated solution for assessing security controls and analyzing and responding to the results of continuous monitoring activities.

Management Response: The Bureau concurs with this recommendation. Our ISCM program was established in response to risk management needs in support of the Bureau's progress towards a holistic risk management approach, the Cross-Agency Priorities that had established ISCM as an objective at that time, as well as doctrine and guidance to include NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September, 2011. Our plans for incremental development and improvement of our ISCM automated capabilities mirrors the research and subsequent conclusions simultaneously performed by the Federal CIO Council as described in the United States Government Concept of Operations (CONOPS) for Information Security Continuous Monitoring. The Bureau analyzed doctrine, guidance and the placement of continuous monitoring in our enterprise based upon our risk assessments and continuous authorization model, and selected elements via a "bottom-up" approach that affords us ISCM return on investment with alignment to our risk mitigation and management needs. Going forward, incremental improvements to the automated tools will continue to increase value in our risk management domain.

Recommendation 2: Assess the ISCM implementation options and guidance outlined in the CONOPS and update the CFPB's ISCM strategy, as necessary.

Management Response: The Bureau concurs with this recommendation. Our ISCM strategy capitalizes on the research and recommendations offered in the CONOPS, and aligns closely to the Iterative and Incremental Model via the DHS CDM BPA option as described in the CONOPS. To this end, the Bureau is actively engaged in the Continuous Diagnostics and Mitigation (CDM) program having executed a Memorandum of Agreement between DHS and the Bureau and closely monitoring the program as it evolves. Given the pressing need for relevant technologies and the schedule for CDM procurements, the Bureau is pressing forward with internal capabilities that will be deployed with a Continuous Monitoring module configured so as to integrate with internal scanning and monitoring tools and vulnerability management solutions. This will allow us to integrate the totality of our security lifecycle and system portfolio, with live data from not only the CDM and dashboard but also our own internal tools resulting in Continuous Monitoring across the CFPB technology enterprise. As the Bureau and its technology enterprise evolve and mature, so too will the ISCM strategy to ensure alignment and effectiveness of the program.

Recommendation 3: Strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.

Response: CFPB concurs with this recommendation. Our plans to continue the evolution of vulnerability management in our enterprise are underway, and on-track for further improvements in FY2015. Enhancements to our vulnerability management tool suite are underway with additional modules and capabilities that enable the Bureau to detect and discern potential issues throughout the enterprise and including, among other, the database and application level. The technology will capitalize on the work already accomplished and noted in your report to standardize system build and configurations to establish a sound baseline operating environment. We intend to further our use of standards-based reference data as provided by the National Vulnerability Database via Common Vulnerabilities and Exposures (CVE) and other SCAP (Security Content Automation Protocol) protocols. During our on-going phased deployments, we are maturing our processes and tools to further the use of SCAP and live content feeds from official sources, thus reducing the time it takes to detect (and then mitigate) security problems in our systems.

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