



OFFICE OF INSPECTOR GENERAL

Audit Report

2015-IT-C-020

# 2015 Audit of the CFPB's Information Security Program

November 13, 2015

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

## Report Contributors

Khalid Hasan, Senior OIG Manager  
Joshua Dieckert, Project Lead  
Paul Vaclavik, Senior IT Auditor  
Daniel Megalo, IT Auditor  
Morgan Fletcher, IT Auditor  
Peter Sheridan, Assistant Inspector General for Information Technology

## Abbreviations

---

|            |  |
|------------|--|
| CFPB       | Consumer Financial Protection Bureau   |
| CIO        | Chief Information Officer  |
| ConOps     | <i>United States Government Concept of Operations for Information Security Continuous Monitoring</i>                             |
| DHS        | U.S. Department of Homeland Security   |
| FISMA      | Federal Information Security Modernization Act of 2014   |
| FY         | fiscal year  |
| IT         | information technology   |
| IG         | Inspector General  |
| ISCM       | information security continuous monitoring   |
| NIST       | National Institute of Standards and Technology   |
| OIG        | Office of Inspector General  |
| SP 800-46  | Special Publication 800-46, <i>Guide to Enterprise Telework and Remote Access</i>  |
| SP 800-50  | Special Publication 800-50, <i>Building an Information Technology Security Awareness and Training Program</i>                    |
| SP 800-61  | Special Publication 800-61, Revision 2, <i>Computer Security Incident Handling Guide</i>   |
| SP 800-100 | Special Publication 800-100, <i>Information Security Handbook: A Guide for Managers</i>  |
| SP 800-128 | Special Publication 800-128, <i>Guide for Security-Focused Configuration Management of Information Systems</i>                   |
| SP 800-137 | Special Publication 800-137, <i>Information Security Continuous Monitoring for Federal Information Systems and Organizations</i> |
| Treasury   | U.S. Department of the Treasury  |

---



# **Executive Summary:**

## **2015 Audit of the CFPB's Information Security Program**

2015-IT-C-020

November 13, 2015

### **Purpose**

To meet our annual Federal Information Security Modernization Act of 2014 (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 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 2015. The guidance directs IGs to evaluate the performance of agencies' information security programs across 10 areas. Also referenced in the guidance is a new maturity model for IGs to use in assessing their agencies' information security continuous monitoring (ISCM) programs.

### **Findings**

The CFPB continues to mature its information security program and ensure that it is consistent with the requirements of FISMA. This year, the CFPB completed transitioning its information technology infrastructure and network services from the U.S. Department of the Treasury and assumed most of the operational responsibilities for information security that were previously shared. In addition, 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 9 out of 10 areas: ISCM, configuration management, identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access, contingency planning, and contractor systems. For the remaining area—security training—as we also noted in 2014, we found that the CFPB had not developed and implemented a role-based training program for individuals with key information security responsibilities.

While we found the CFPB's information security program to be consistent with requirements outlined in DHS's FISMA reporting guidance for ISCM, configuration management, incident response, and remote access, we identified opportunities to strengthen controls in these areas. Specifically, we identified improvements needed to mature the CFPB's ISCM program in the areas of people, processes, and technology through greater centralization and automation. In addition, our 2013 and 2014 FISMA audit reports include six recommendations to strengthen the CFPB's ISCM, configuration management, incident response, and security training programs by improving planning, leveraging automation, and increasing centralization. We found that the agency was in the process of taking actions to close these recommendations.

We also identified improvements needed in the CFPB's information security policy and remote access management processes. Specifically, we found that the CFPB had not ensured that its information security policies and procedures were updated in a timely manner to address changing risks and federal requirements. We also found that the CFPB was using an outdated encryption mechanism to secure remote access to its information technology infrastructure.

### **Recommendations**

Our report includes two new recommendations to strengthen the CFPB's information security policy and remote access management processes. These recommendations are designed to (1) ensure that security policies, procedures, and guidance are updated in a timely manner and (2) strengthen the cryptographic mechanism employed for the CFPB's remote access solution in accordance with National Institute of Standards and Technology guidance. In his response to our report, the Chief Information Officer concurs with our recommendations and outlines actions that have been taken, are underway, and are planned to strengthen the CFPB's information security program.

### Summary of Recommendations, OIG Report No. 2015-IT-C-020

| Rec. no. | Report page no. | Recommendation  | Responsible office                      |
|----------|-----------------|---|---|
| 1        | 11              | Ensure that the CFPB's information security policy, procedure, standard, and process documents are periodically updated to reflect the security requirements, processes, and technologies currently in place. | Office of the Chief Information Officer |
| 2        | 12              | Strengthen the cryptographic mechanism employed for the CFPB's remote access solution in accordance with National Institute of Standards and Technology guidance.   | Office of the Chief Information Officer |



## OFFICE OF INSPECTOR GENERAL

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

November 13, 2015

### MEMORANDUM

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

**FROM:** Peter Sheridan *Peter Sheridan*  
Assistant Inspector General for Information Technology

**SUBJECT:** OIG Report No. 2015-IT-C-020: *2015 Audit of the CFPB's Information Security Program*

The Office of Inspector General (OIG) is pleased to present its report on the 2015 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 Modernization Act of 2014, which requires each agency Inspector General to conduct an annual independent evaluation of the effectiveness of the agency's information security program and practices. As part of this audit, we also reviewed security controls for a select agency system. The detailed results of our review of the security controls for this system 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 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*.

Our report contains recommendations designed to ensure that security policies, procedures, and guidance are updated in a timely manner and strengthen the cryptographic mechanism employed for the CFPB's remote access solution in accordance with National Institute of Standards and Technology guidance. We provided a draft of our report to you for review and comment. In your response, you note that actions have been taken, are underway, and are planned to address our recommendations. We have included your response as appendix B to our report.

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  
Stephen Agostini, Chief Financial Officer  
Zachary Brown, Chief Information Security Officer  
J. Anthony Ogden, Deputy Inspector General

# Contents

|  |    |
|--|----|
| <b>Introduction</b> .....  | 1  |
| Objectives .....   | 1  |
| Background.....  | 1  |
| <b>Summary of Findings</b> .....   | 2  |
| <b>Analysis of the CFPB’s Progress in Implementing Key FISMA and<br/>DHS Information Security Program Requirements</b> ..... | 3  |
| Information Security Continuous Monitoring .....   | 3  |
| Configuration Management.....  | 6  |
| Incident Response and Reporting .....  | 8  |
| Security Training.....   | 9  |
| Policies and Procedures .....  | 10 |
| Remote Access .....  | 11 |
| <b>Appendix A: Scope and Methodology</b> .....   | 13 |
| <b>Appendix B: Management’s Response</b> .....   | 14 |

# Introduction

## Objectives

Our specific audit objectives, based on the requirements of the Federal Information Security Modernization Act of 2014 (FISMA),<sup>1</sup> 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. 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 the effectiveness of information security policies, procedures, and practices for select systems.

In support of FISMA's independent evaluation requirements, the U.S. Department of Homeland Security (DHS) issued guidance to IGs on FISMA reporting for 2015.<sup>2</sup> This guidance directs IGs to evaluate the performance of agency information security programs across a variety of attributes grouped into 10 areas. These areas are information security continuous monitoring (ISCM), configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems.

As noted in our prior FISMA audit reports, 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). However, as of August 2015, the CFPB has transitioned these resources from Treasury and is managing its information technology (IT) infrastructure and network. With this transition completed, the CFPB's information security program is now largely operating independently of Treasury; however, the agency continues to share with Treasury operational responsibilities for security awareness training. CFPB officials informed us that the agency plans to continue to use Treasury's services for security awareness training.

---

1. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-228, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–58).

2. U.S. Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, June 19, 2015.

# Summary of Findings

The CFPB continues to mature its information security program and ensure that it is consistent with FISMA requirements. For instance, the agency completed migration of its IT infrastructure from Treasury, began implementation of tools to automate several security processes, and strengthened its enterprise-wide risk and incident management processes. In addition, 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 9 out of 10 information security areas: ISCM, configuration management, identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access, contingency planning, and contractor systems. For the remaining area—security training—as we also noted in 2014, we found that the CFPB had not developed and implemented a role-based training program for individuals with key information security responsibilities.

While we found the CFPB's information security program to be consistent with requirements outlined in DHS's FISMA reporting guidance for IGs in the areas of ISCM, configuration management, incident response and reporting, and remote access management, we identified opportunities to strengthen controls in these areas. We identified steps that the CFPB should take to mature its ISCM program in the areas of people, processes, and technology through greater centralization and automation. Specifically, to implement an effective ISCM program, we found that the agency should (1) prioritize development of a role-based security training program that covers the ISCM processes and technologies used at the agency, (2) update its ISCM strategy to reflect the processes and technologies the agency plans to use to meet ISCM requirements, (3) develop a formal lessons-learned process for its ISCM program, and (4) fully implement automated solutions for strengthening inventory controls over IT assets, assessing security controls, and analyzing and responding to the results of continuous monitoring activities.

In addition, our 2013 and 2014 FISMA audit reports include six recommendations to strengthen the CFPB's ISCM, configuration management, incident response, and security training programs by improving planning, leveraging automation, and increasing centralization. We found that the agency was in the process of taking actions to close these recommendations. As such, our recommendations in these areas remain open, and we will follow up on their status as part of our future FISMA audits.

We also identified improvements needed in the CFPB's information security policy and remote access management processes. Specifically, we found that the CFPB had not ensured that its information security policies, procedures, standards, and process documents were updated to address changing risks and federal requirements. This specifically affects several components of the CFPB's information security program, including ISCM, incident response, and continuity of operations. We also found that the CFPB was using outdated cryptographic technologies to secure remote access to its IT infrastructure. This cryptographic technology was not approved by the National Institute of Standards and Technology (NIST) for use in federal information systems due to the presence of known security vulnerabilities.



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

## Information Security Continuous Monitoring

### ***Requirement***

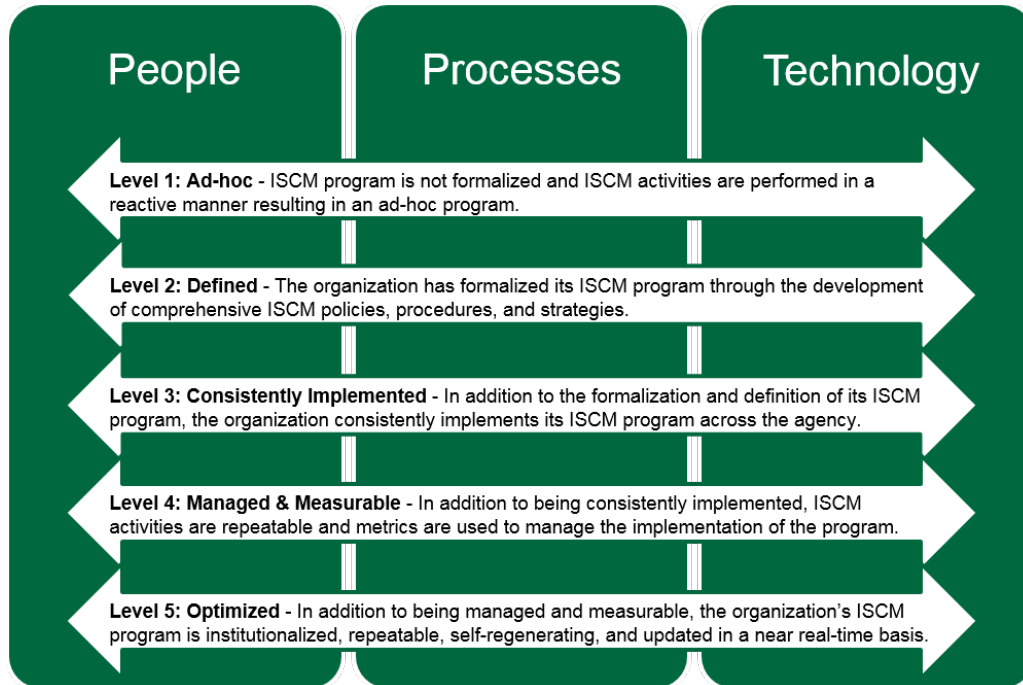
ISCM has been designated by the Office of Management and Budget as a cross-agency priority goal, with the intent to transform the historically static security control assessment and authorization process into an integral part of a dynamic enterprise-wide risk management process.<sup>3</sup> Best practices for implementing ISCM are outlined in NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (SP 800-137). SP 800-137 defines ISCM as the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. In addition, SP 800-137 notes that when an ISCM program is first implemented, there will likely be several aspects of the organization's security program that are manually monitored, with capabilities expanding and maturing over time. This maturity in security is implemented through a combination of people, processes, and technology.

To provide a greater perspective on the overall status of agencies' ISCM programs, the Council of the Inspectors General on Integrity and Efficiency, in coordination with DHS, the Office of Management and Budget, and other stakeholders, developed an ISCM maturity model for use by IGs as part of their fiscal year (FY) 2015 FISMA reviews. Referencing existing ISCM requirements, the maturity model includes steps to assess an agency's continuous monitoring program through an analysis of three domains: people, processes, and technology. The maturity levels of each of these domains dictate the overall maturity of an organization's ISCM program. Specifically, as noted in the DHS's FY 2015 FISMA reporting guidance for IGs, the "lowest common denominator" approach shall apply when determining the overall maturity level for an organization's ISCM program. For instance, if an organization is at level 1 for the *people* domain but at level 3 for both the *processes* and *technology* domains, the overall maturity of the organization's ISCM program would be level 1. Figure 1 provides an overview of the five maturity levels of the ISCM maturity model.

---

3. The cross-agency priority goals were introduced in the fiscal year 2013 federal budget and focus on 14 major issues that run across several federal agencies.

**Figure 1: Information Security Continuous Monitoring Maturity Model**



Source: Office of Inspector General analysis of DHS's FY 2015 FISMA reporting guidance for IGs.

### ***Progress to Date***

We found that the CFPB has taken several steps to develop and implement an ISCM program that is consistent with SP 800-137 and the ISCM maturity model. For instance, from a people perspective, the CFPB has developed and implemented components of its ISCM policy and supporting procedures that include the roles and responsibilities of various stakeholders and processes for information sharing in support of risk-based decisionmaking. In addition, the CFPB has defined and implemented processes for ongoing assessments and monitoring of security controls, as well as for integrating ISCM with risk management activities. Further, the agency has implemented several technologies to support ISCM activities and has identified solutions it plans to implement for all automation areas outlined in SP 800-137.<sup>4</sup>

### ***Work to Be Done***

We found that the CFPB's ISCM program is operating at level 1, with the agency performing several, but not all, recommended activities indicative of higher maturity levels. Overall, consistent with the findings outlined in our 2014 FISMA audit report, we found that by updating its ISCM strategy to comprehensively define all ISCM processes and by increasing the use of automation and centralization, the CFPB can better ensure the effectiveness of its ISCM

4. The 11 automation areas outlined in SP 800-137 are patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management.

program.<sup>5</sup> The following sections provide additional details on the maturity of the CFPB's ISCM program by domain, including the steps we believe that the agency should prioritize in the next year to continue to mature its ISCM program.

## **People**

We found that the people domain of the CFPB's ISCM program was operating at level 2, with roles and responsibilities defined and communicated across the organization. We noted that to reach level 3 for the people domain, the CFPB should prioritize improving its processes for ensuring that personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. As detailed later, the CFPB has not developed and implemented a role-based security training program that includes the ISCM processes and technologies used at the agency. Once this training program is implemented, and in conjunction with improvements in the processes and technology domains outlined below, it could further assist the CFPB in ensuring that the rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization.

## **Processes**

We found that the processes domain of the CFPB's ISCM program was operating at level 1, with some ISCM processes defined and implemented. In our 2014 FISMA audit report, we recommended that the Chief Information Officer (CIO) assess the ISCM implementation options and guidance outlined in the United States Government Concept of Operations for Information Security Continuous Monitoring (ConOps) and update the CFPB's ISCM strategy, as necessary. As part of our follow-up work, we found that the agency's ISCM strategy is still being updated to better align with the processes and technologies outlined in SP 800-137, DHS's Continuous Diagnostics and Mitigation program, as well as the ConOps. Therefore, our recommendation in this area remains open, and we will monitor the CFPB's efforts as part of future FISMA audits.

We also found that the CFPB's ISCM program does not incorporate a formal lessons-learned process to facilitate ongoing improvements in the program. While the agency has designated an ISCM lead who acquires feedback from participants and stakeholders, this practice is performed informally and with little to no documentation. As the CFPB continues to automate its ISCM program, a formal, documented lessons-learned process can provide timely and relevant feedback to improve the agency's ISCM capabilities as well as further engage the program's stakeholders.

In addition, during our fieldwork, the agency's external financial statement audit and a subsequent internal review performed by the CFPB identified several improvements needed to the agency's hardware asset management processes. As noted in DHS' FY 2015 FISMA reporting guidance for IGs, asset management is one of the first areas in which ISCM processes should be developed. Specifically, organizations must first know about the devices and software

---

5. NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, notes that in the context of information security, *effectiveness* addresses the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements or enforcing established security policies. In line with this definition, level 3 in the ISCM maturity model represents an effective ISCM program.

installed on their network before they can manage the configurations and vulnerabilities of those devices and software. CFPB officials informed us that the agency is taking several actions to define, standardize, and automate its processes for hardware asset management.

## ***Technology***

We found that the technology domain of the CFPB's ISCM program was operating at level 2. The technologies that the CFPB plans to use to perform ISCM have been defined but not consistently implemented. For instance, our 2014 FISMA audit report included a recommendation for the CIO to fully implement the agency's selected automated solution for assessing security controls and analyzing and responding to the results of continuous monitoring activities. In 2015, we found that the automated solution has been selected and procured but not implemented across the agency. Therefore, our recommendation in this area remains open, and we will continue to monitor the CFPB's efforts as part of future FISMA audits.

In addition, similar to our findings from 2014, we found that components of the CFPB's ISCM program continue to rely on manual and labor-intensive processes in instances in which automation would be more effective. For example, to complete ongoing control assessments, the CFPB's Cybersecurity Office must first individually reach out to system security officials across the organization 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 by the ISCM lead 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. Further, as noted above, hardware asset management was identified as an improvement area during the agency's external financial statement audit as well as a subsequent internal review performed by the CFPB. CFPB officials informed us that the agency is in the process of implementing an automated solution to help standardize and automate its processes for hardware asset management.

## **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. In addition, SP 800-128 highlights the importance of using automated tools to scan different system components (e.g., Web server, database server, and network devices) to manage security configurations. SP 800-128 further notes 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 taken several steps to implement a configuration management program that is consistent with FISMA and SP 800-128. For instance, the agency has developed configuration baselines for all major technologies used at the agency and implemented a patch management process. We conducted vulnerability scanning on select CFPB IT devices and noted improvements in the installation of patches at the operating system and application levels. Further, with the transition of its IT infrastructure and network from Treasury complete, the agency has deployed its own laptop image that is configured in accordance with the *United States Government Configuration Baseline* guidance.

### ***Work to Be Done***

As part of our 2014 FISMA audit, we recommended 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. While we found improvements in the implementation of security settings from last year at the application level, our vulnerability scanning identified vulnerabilities as well as configuration settings at the database level that did not align with the agency's baselines. For example, we found that the latest database-level patch set, which included fixes for several vulnerabilities, was not applied for a server maintaining several databases. In addition, for this server, we identified configurations related to audit logging and password management that were not aligned with the agency's baseline.

The CFPB is currently relying on an automated solution to perform vulnerability scanning; however, this solution offers limited visibility to the database and application levels of the agency's IT environment. By implementing an automated solution that is targeted toward managing vulnerabilities at the application and database levels, the agency can obtain greater assurance that its systems are securely configured to protect against known vulnerabilities. Therefore, our 2014 recommendation in this area remains open, and we will continue to monitor the CFPB's efforts in this area as part of our future FISMA audits.

In addition, as part of our 2013 FISMA audit, we recommended that the CFPB develop and implement an organization-wide configuration management plan. In 2014 and again this year, we found that the CFPB had not completed development of this plan. The delay in developing and implementing a configuration management plan can be attributed to the challenges associated with migrating all the CFPB's IT infrastructure and network components from Treasury. With this transition now completed, the development and implementation of an organization-wide configuration management plan can help ensure that all components of CFPB systems are securely configured. Therefore, our 2013 recommendation in this area remains open, and we will continue to monitor the CFPB's efforts in this area as part of our future FISMA audits.

# 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***

The CFPB has taken several steps to strengthen its capability to detect, report, and respond to security incidents. For instance, with the transition of its IT infrastructure and network from Treasury completed, the agency has established a computer security incident response team and supporting processes for reporting applicable computer security incidents directly to the United States Computer Emergency Readiness Team. The CFPB has also deployed intrusion detection systems at its major network access points, and it is in the process of deploying an automated solution to perform centralized audit monitoring and incident correlation functions.

## ***Work to Be Done***

In our 2013 FISMA report, we recommended that the CIO ensure that audit logs and security incident information from all relevant sources are centrally tracked, analyzed, and correlated. In 2014, we found that the CFPB was in the process of procuring an automated tool to provide these capabilities. This year, we found that the CFPB had selected and procured an automated tool and was configuring it for deployment. As such, incident correlation continues to be a manual, time-intensive process.

The delay in implementing an automated solution can be attributed to the challenges associated with migrating all the CFPB's IT infrastructure and network components from Treasury. Until these infrastructure and network components were transitioned, the CFPB could not easily configure audit logs and security incident information from these devices to be automatically reported to a centralized monitoring tool. Once it is effectively implemented, the CFPB's automated solution for centrally tracking, analyzing, and correlating information about incident activity will help ensure that the CFPB can fully detect and respond to information security incidents in a timely manner. Therefore, our 2013 recommendation in this area remains open, and we will continue to follow up on the CFPB's efforts as part of our future FISMA audits.

## Security Training

### ***Requirement***

FISMA requires agencies to provide security awareness training to all information system users and provide 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 educating all users about overall information security policies, while the latter is geared toward teaching information security skills needed to perform specific IT 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 IT security awareness and training program: program design, development, implementation, and post-implementation.

### ***Progress to Date***

The CFPB has developed and implemented a security awareness training program that is consistent with SP 800-50 and other best practices. The agency 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. We also found that the CFPB is using DHS's Federal Virtual Training Environment, an online and on-demand cybersecurity training system, to help its workforce maintain expertise and to foster operational readiness.

### ***Work to Be Done***

In our 2013 FISMA report, we recommended that the CIO design, develop, and implement a role-based security training program for individuals with significant information security responsibilities. In 2014, we kept our recommendation open, and this year we again found that the CFPB had not designed, developed, and implemented a role-based security training program for individuals with key information security responsibilities. Specifically, we found that the CFPB had not conducted an assessment to determine its role-based security training needs and define which roles within the agency require such training, developed a role-based security training strategy and plan, and established a role-based security training curriculum.

We believe that the CFPB delayed work on creating a role-based training program due to resource constraints and because it was evaluating options to combine security and privacy role-based training offerings. In addition, the CFPB hired a security awareness and training specialist in July 2015, and this individual noted that the CFPB plans to conduct in-house role-based training in 2016. 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. Accordingly, our 2013

recommendation in this area remains open, and we will continue to monitor the CFPB's efforts as part of our future FISMA audits.

## **Policies and Procedures**

### ***Requirement***

FISMA requires each agency to develop and maintain information security policies and procedures to address the requirements of the legislation and of other federal standards. Best practices for information security governance, including policy management, are referenced in NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers* (SP 800-100). SP 800-100 notes that agency information security policies are an essential component of information security governance that should be continually reviewed to ensure that they are aligned with evolving technologies and federal requirements. SP 800-100 further states that over time, policies and procedures can become inadequate because of changes in the agency's business processes, threat environment, and technology infrastructure. To manage these changes, NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires agencies to develop a review process that ensures that the agency's security policies, procedures, and practices accurately reflect any new or evolving risks, requirements, and changes to the organization.

### ***Progress to Date***

The CFPB has developed and implemented multiple information security policies, procedures, standards, and processes. To manage these artifacts, the CFPB has developed a process for the development, approval, dissemination, and maintenance of its information security policies, standards, and processes. This process requires the agency to periodically review and update information security policy, procedure, standards, and process documentation to ensure that the content remains current and accurate. Further, the process includes the use of an internal status tracker to document any updates, revisions, and approvals to information security policy-related documentation. The tracker is to be maintained on a weekly basis to reflect which stage in the development and review process each policy, standard, and process document is in.

### ***Work to Be Done***

We found that several of the CFPB's policy, procedure, standard, and process documents had not been regularly reviewed and updated in accordance with the organization's defined review process. As a result, several of these documents contain information that is out-of-date with federal requirements as well as changes in the technology, infrastructure, and business processes of the agency. For example, the CFPB's *Access Control Process* document describes the use of Treasury's process for access provisioning and deprovisioning. However, the agency has transitioned its IT infrastructure and network operations from Treasury, and CFPB officials informed us that the agency has been performing its own account management activities. We also found that many of the points of contact in these documents are outdated, including several contacts necessary for activating the agency's continuity of operations plan.



We believe that a key reason for these issues is that the CFPB was focusing its operational resources on the transition of IT and security services from Treasury. With the transition of its IT infrastructure and network from Treasury completed, updated security policy, procedures, standards, and process documentation could provide the CFPB with additional assurance that it is managing information security risks in accordance with federal and agency requirements.

## **Recommendation**

We recommend that the CIO

1. Ensure that the CFPB's information security policy, procedure, standard, and process documents are periodically updated to reflect the security requirements, processes, and technologies currently in place.

## **Management's Response**

In his response to our report, the CIO concurs with this recommendation and states that the agency is taking actions to strengthen its cybersecurity publication management life cycle and implement a new tracking and review process. In addition, the CIO notes that the CFPB has appointed a new employee to lead its program management team that is responsible for addressing this recommendation.

## **OIG Comment**

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

## **Remote Access**

### **Requirement**

*Remote access* refers to the ability of an authorized user (or information system) to access an organization's nonpublic information systems by communicating through an external, non-organization controlled network (e.g., the Internet). DHS's FY 2015 FISMA reporting guidance for IGs notes that remote connections over the Internet provide opportunities for compromise of information in transit, and thus, they need compensating controls to ensure that only properly identified and authenticated users gain access and that the connections prevent hijacking by others.

Best practices for selecting, implementing, and maintaining security controls for remote access solutions are outlined in NIST Special Publication 800-46, *Guide to Enterprise Telework and Remote Access* (SP 800-46). SP 800-46 notes that a key component of ensuring the confidentiality and integrity of remote access connections is the use of cryptography, which is a method for transforming data to hide its content. Federal agencies are required to use cryptographic algorithms that are approved by NIST.

## ***Progress to Date***

The CFPB has developed a telework program that allows staff to work at preapproved locations other than their official worksite. With the transition of its IT infrastructure and network from Treasury completed, the CFPB now manages its own remote access solution, which enables staff to interface with the organization's nonpublic computing resources. To monitor external Internet connections, the CFPB has contracted with a third-party service provider. Further, the agency has entered into an agreement with DHS for additional network monitoring services, including intrusion protection services, to monitor network traffic for known or suspected malicious cyber activity.

## ***Work to Be Done***

While we found that the CFPB employs several controls to secure its remote access connections, we identified opportunities to strengthen the encryption mechanisms being used for remote access to its IT infrastructure. Specifically, we found that the CFPB had not updated the cryptographic mechanism employed for its remote access solution in accordance with NIST requirements. CFPB officials informed us that adequate planning had not been performed to ensure that these requirements were met. We believe that strengthening controls, in accordance with NIST requirements for securing communications, will provide greater assurance that the CFPB is able to mitigate risks to the confidentiality and integrity of its data that are accessed remotely.

## ***Recommendation***

We recommend that the CIO

2. Strengthen the cryptographic mechanism employed for the CFPB's remote access solution in accordance with NIST guidance.

## ***Management's Response***

In his response to our report, the CIO concurs with this recommendation and states that the CFPB has developed a course of action to address interoperability and legacy compatibility issues that may arise during the remediation of this issue.

## ***OIG Comment***

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

# Appendix A

## 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 10 areas outlined in DHS's FY 2015 FISMA reporting guidance for IGs. These areas are ISCM, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems. 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 an agency system and performed vulnerability scanning at the operating system, database, and application levels on select IT devices.

We used 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 FY 2015 FISMA reporting guidance for IGs. As noted in our report, the CFPB's information security program is largely operating independently; however, the agency continues to rely on Treasury for security awareness training. As part of our assessment of the CFPB's security awareness training program, we determined whether the Treasury OIG had identified any issues with regard to Treasury's security awareness processes that would affect the CFPB. We also met with the agency's external financial statement auditor.

We performed our fieldwork from June 2015 to October 2015. 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.

# Appendix B

## Management's Response



1700 G Street NW, Washington, DC 20552

November 11, 2015

Mr. Peter Sheridan  
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 *2015 Audit of the CFPB's Information Security Program*.

We are pleased that you found that the Bureau continues to mature our FISMA compliance and Information Security posture. The report noted the completion of our project to transition our technology infrastructure and network services from the Department of Treasury. The Bureau is now sustaining our own Trusted Internet Connection (TIC)-compliant network access through a Managed Trusted Internet Protocol Service (MTIPS) service provider. We are also autonomously operating our Computer Security Incident Response Team, and have completed our liaison agreements with U.S. CERT. Now that the Bureau is operating our enterprise information technology independently from Treasury, we look forward to continuing the cybersecurity improvements to our infrastructure over the next year.

We appreciate you noting that we have continued to mature our information security program and are ensuring that the Bureau's information security program is consistent with FISMA. As your report points out, in addition to the completion of our independence project, the Bureau is strengthening our enterprise-wide risk and incident management capability. Our enterprise logging infrastructure is now in place, as is our Security Information and Event Management solution. Once fully implemented, this infrastructure will fuse information from sensors, firewalls, and other security mechanisms with audit log and other relevant information, allowing the Bureau to improve our incident detection and response capability, while informing the totality of continuous monitoring and ongoing enterprise risk management.

[consumerfinance.gov](http://consumerfinance.gov)

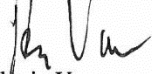
The Bureau is pleased to note that amidst the transition of infrastructure and support, you now record us as consistent with nine of the ten OIG FISMA areas, specifically Information Security Continuous Monitoring (ISCM), configuration management, identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access, contingency planning, and contractor systems. In FY16, we will be working to incrementally improve and mature our processes in the security training domain, with a focus on role-based training for persons with significant security responsibilities. We have already completed identifying those roles, defining the training plan for each, and are in the process of finalizing the implementation plan. When implemented in FY16, it will be a key element of our security education, training, and awareness domain. We will continue to take steps to mature our capabilities in this FISMA area.

In your report, you noted our progress not only in ISCM, but in configuration management, incident response, and remote access. We acknowledge and agree with your observations related to the maturation of our ISCM program. Our role-based security training program will also include ISCM roles and responsibilities. As part of our ISCM evolution, we continue to update our strategy and to complete the deployment of a software platform that will assist us in automating much of the ISCM and incident reporting efforts. Noting the evaluation criteria of the new ISCM maturity model that served as the basis for your assessment, we will be capturing “lessons learned” during these projects as well as the initial operating capability, and use them to inform our prioritization and resource allocation decision-making in support of ISCM.

We appreciate the status on the prior year recommendations and will continue to work to bring them to closure. We have already taken steps to increase Cybersecurity’s capabilities to retroactively correct matters related to previous recommendations while supporting the expansion of new and improved consumer services in a secure and compliant manner. We will continue with the remediation efforts in fiscal year 2016.

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

Sincerely,



Ashwin Vasan  
Chief Information Officer

[consumerfinance.gov](http://consumerfinance.gov)

**Response to recommendations presented in the Draft IG Report,  
“2015 Audit of the CFPB’s Information Security Program.”**

*Recommendation 1:* Ensure that the CFPB’s information security policy, procedures, standards, and process documents are periodically updated to reflect the security requirements, processes, and technologies currently in place.

*Management Response:* The Bureau concurs with this recommendation. As you noted in your report, the Bureau had to focus significant resources on the transition activities related to our Treasury independence project. We are already revamping our Cybersecurity publication management lifecycle, instantiating a new tracking and review/revise timing process, and developing improvements to the layout and design of how control requirements and control measures are represented and codified in our publications. These changes and the appointment of a new federal employee as the lead for the Cybersecurity Program Management team are helping us to ensure we are poised to address this recommendation in the coming year.

*Recommendation 2:* Strengthen the cryptographic mechanism employed for the CFPB’s remote access solution in accordance with NIST requirements.

*Management Response:* The Bureau concurs with this recommendation. We are aware of the various standards and requirements that focus on cryptographic protections, and the evolving NIST body of publications that define everything from protocols to ciphers and key sizes. In the course of evolving our infrastructure, we do have to address interoperability and legacy compatibility issues. The Bureau has determined a course of action to remediate this matter, and will be implementing it in a timely manner.

consumerfinance.gov



## 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](http://www.federalreserve.gov/oig)  
or  
[www.consumerfinance.gov/oig](http://www.consumerfinance.gov/oig)