OFFICE OF INSPECTOR GENERAL

Audit Report 2016-IT-C-012

2016 Audit of the CFPB's Information Security Program

November 10, 2016

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

Report Contributors

Khalid Hasan, Senior OIG Manager
Andrew Gibson, OIG Manager
Joshua Dieckert, Project Lead
Amanda Sundstrom, IT Auditor
Rebecca Kenyon, IT Auditor
Kaneisha Johnson, IT Auditor
Peter Sheridan, Assistant Inspector General for Information Technology

Abbreviations

BIA	business impact analysis
CDM	Continuous Diagnostics and Mitigation
CFPB	Consumer Financial Protection Bureau
CIO	Chief Information Officer
COOP	continuity of operations plan
DHS	U.S. Department of Homeland Security
DLP	data loss prevention
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
IG	Inspector General
IR	incident response
ISCM	information security continuous monitoring
IT	information technology
ITCP	information technology contingency plan
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	personal identity verification
ROB	rules of behavior
SP 800-34	Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
SP 800-61	Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*
SP 800-137	Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
Treasury	U.S. Department of the Treasury
UAF	user access form
US-CERT	United States Computer Emergency Readiness Team

Executive Summary:

2016 Audit of the CFPB's Information Security Program

2016-IT-C-012 November 10, 2016

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 (1) security controls and techniques and (2) information security policies, procedures, and practices.

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 has issued guidance to the IGs on FISMA reporting for 2016. The guidance directs the IGs to evaluate the performance of agencies' information security programs across eight domains that are grouped into five function areas: identify, protect, detect, respond, and recover. Also referenced in the guidance is a maturity model for the IGs to use in assessing their agencies' information security continuous monitoring (ISCM) and incident response programs.

Findings

The CFPB continues to mature its information security program to ensure that it is consistent with FISMA requirements. For instance, the CFPB implemented several tools to automate ISCM capabilities, matured its ISCM program from level 1 (*ad hoc*) to level 3 (*consistently implemented*), and strengthened its role-based training program for users with significant security responsibilities. In addition, the CFPB's information security program is generally consistent with seven of eight U.S. Department of Homeland Security information security domains: risk management, contractor systems, configuration management, identity and access management, security and privacy training, ISCM, and incident response. For the remaining domain of contingency planning, the CFPB has not completed an agency-wide business impact analysis to guide its contingency planning activities, nor has it fully updated its continuity of operations plan to reflect the transition of its information technology infrastructure from the U.S. Department of the Treasury.

In addition, while the agency's information security program was generally consistent with requirements outlined in the U.S. Department of Homeland Security's FISMA reporting guidance for IGs in risk management and identity and access management, the CFPB can strengthen controls in those areas to ensure that they are effective. Specifically, the CFPB can strengthen its risk management program by formalizing its insider threat activities and evaluating options to develop an agency-wide insider threat program that leverages planned activities around data loss prevention. Related to the management of insider threat risks, signed rules of behavior documents were not in place for several privileged users who were not consistently resubmitting user access forms to validate the need for their elevated access privileges.

Finally, the CFPB has made further progress in addressing our recommendations from past years' FISMA audit reports. Of 12 total recommendations, 7 remained open at the start of our 2016 FISMA audit. The CFPB has taken sufficient actions to close 6 of the 7 open recommendations.

Recommendations

Our report includes three new recommendations to strengthen the CFPB's information security program: (1) formalize insider threat activities through an agency-wide insider threat program strategy, (2) ensure that user access forms and rules of behavior for privileged users are maintained, and (3) ensure that a business impact analysis is conducted and used to guide contingency planning activities. The Chief Information Officer concurs with our recommendations and has outlined actions that are underway or will be taken to strengthen the CFPB's information security program.

Summary of Recommendations, OIG Report 2016-IT-C-012

Recommendation number	Page	Recommendation	Responsible office
1	7	Evaluate options and develop an agency-wide insider threat program to include a. a strategy to raise organizational awareness. b. an optimal organizational structure. c. integration of incident response capabilities, such as ongoing activities around data loss prevention.	Office of the Chief Information Officer
2	9	Ensure that a. a signed user access form and rules of behavior document is on file and maintained for each privileged user. b. all privileged user accounts are annually recertified.	Office of the Chief Information Officer
3	11	Strengthen the CFPB's contingency program by a. performing an agency-wide business impact analysis. b. updating the agency's continuity of operations plan and information technology contingency plan to reflect the results of the business impact analysis and the current operating environment of the CFPB.	Office of the Chief Information Officer

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

November 10, 2016

MEMORANDUM

TO: Vijay Desai
Acting Chief Information Officer
Consumer Financial Protection Bureau

Sartaj Alag
Chief Operating Officer
Consumer Financial Protection Bureau

FROM: Peter Sheridan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2016-IT-C-012: *2016 Audit of the CFPB's Information Security Program*

The Office of Inspector General has completed its report on the subject audit. 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 our work, we also reviewed security controls for a select agency system; the detailed results of that review will be transmitted under separate, restricted cover. In addition, we will use the results of this audit to respond to specific questions in the U.S. Department of Homeland Security's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

We provided you with a draft of our report for review and comment. In your response, you concur with our recommendations and outline actions that have been or will be taken to address them. We have included your response as appendix C 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: Stephen Agostini, Chief Financial Officer
Zachary Brown, Chief Information Security Officer

Contents

Introduction

Objectives

Our audit objectives, based on Federal Information Security Modernization Act of 2014 (FISMA) requirements, were to evaluate the effectiveness of the Consumer Financial Protection Bureau's (CFPB) (1) security controls and techniques and (2) information security policies, procedures, and practices. Our scope and methodology are detailed in appendix A.

Background

FISMA, which amended the Federal Information Security Management Act of 2002, requires agencies to develop, document, and implement an agency-wide information security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source.[1] FISMA also requires that each agency Inspector General (IG) perform an annual independent evaluation to determine the effectiveness 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 the IGs on FISMA reporting for 2016.[2] This guidance directs the IGs to evaluate the effectiveness[3] of agency information security programs across a variety of attributes grouped into eight security domains: risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring (ISCM), incident response (IR), and contingency planning. These domains map to the five information security functions outlined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity—identify, protect, detect, respond, and recover—as shown in table 1.

1. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551-3558).

2. U.S. Department of Homeland Security, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, September 9, 2016.

3. National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, notes that security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

Table 1: Cybersecurity Framework Security Functions Alignment With the FISMA Metric Domains

Cybersecurity framework security functions	FISMA metric domains
Identify	Risk management and contractor systems
Protect	Configuration management, identity and access management, and security and privacy training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

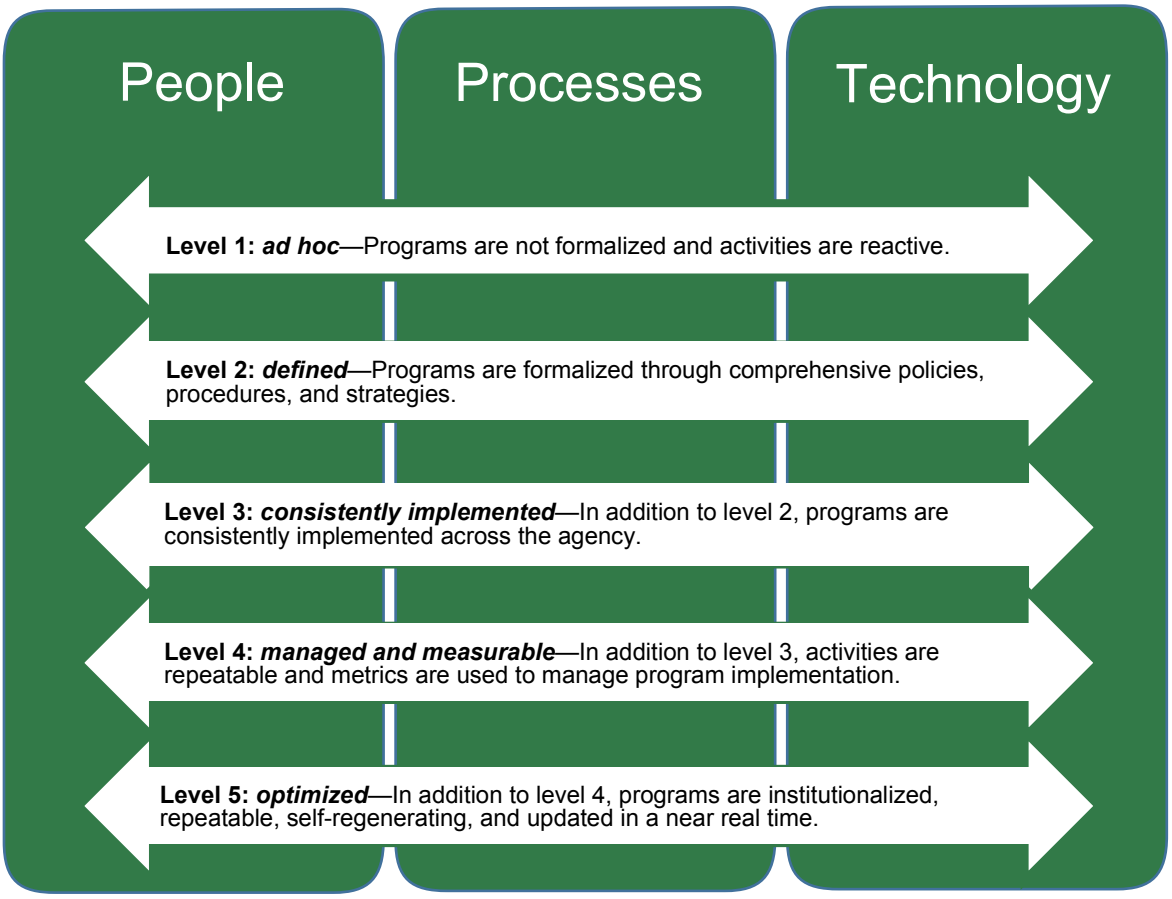
Source: DHS, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

Maturity Model Approach for Assessing Agency Information Security Programs

With the increased focus in FISMA on security control effectiveness, in 2015 the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Office of Management and Budget (OMB), DHS, NIST, and other key stakeholders, undertook an effort to develop a maturity model to evaluate the operating effectiveness of information security programs within a given agency and across agencies. In 2015, DHS's FISMA reporting guidance for IGs included a maturity model for ISCM, a key cybersecurity focus area for the federal government. In 2016, DHS's FISMA reporting guidance for IGs expanded to include a maturity model for IR, another key cybersecurity focus area.

The purpose of the maturity models is (1) to summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) to provide transparency to agency Chief Information Officers, top management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and (3) to help ensure that annual FISMA reviews are consistent across IGs. The maturity model includes steps to assess an agency's 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 program. Figure 1 on the next page provides an overview of the five levels of the maturity model. A maturity ranking of level 4 represents an effective level of security within an area.

Figure 1: Maturity Model Rating Scale



Source: OIG analysis of DHS's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

Summary of Findings

The CFPB continues to mature its information security program and ensure that it is consistent with FISMA requirements. The agency has implemented several tools to automate ISCM capabilities, matured its ISCM program from level 1 (*ad hoc*) to level 3 (*consistently implemented*), and strengthened its role-based training program for users with significant security responsibilities. 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 seven of eight information security areas: risk management, contractor systems, configuration management, identity and access management, security and privacy training, ISCM, and IR. For the remaining area—contingency planning—we found that the agency has not completed an agency-wide business impact analysis (BIA) to guide its contingency planning activities and its continuity of operations plan (COOP) does not reflect the agency's current information technology (IT) operating environment.

We also identified improvements needed in the CFPB's risk management and identity and access management programs. Given the recent threat environment and increased governmentwide focus on insider threats, the CFPB should formalize its insider threat activities and evaluate options to develop an agency-wide insider threat program that leverages planned activities around data loss prevention (DLP). We identified improvements to controls for the agency's privileged IT users, such as system and database administrators, to better manage risks from insider threats. Specifically, we found that rules of behavior for these users were not consistently maintained and user access forms were not being resubmitted to validate the need for elevated privileges.

In addition, although the CFPB's information security program is consistent with requirements outlined in DHS's FISMA reporting guidance for IGs in the areas of ISCM and IR, we determined that the agency can mature those areas by strengthening processes related to developing and implementing security metrics and further centralizing and automating such activities as DLP.

In addition, our prior years' FISMA audit reports included 12 total recommendations, 7 of which remained open at the start of our 2016 FISMA audit. These recommendations were related to ISCM, configuration management, security training, IR, policies and procedures, and remote access. The CFPB has taken sufficient actions to close 6 of the 7 open recommendations. We are leaving our 2014 recommendation related to configuration management open and will follow up on its status as part of our future FISMA audits.[4]

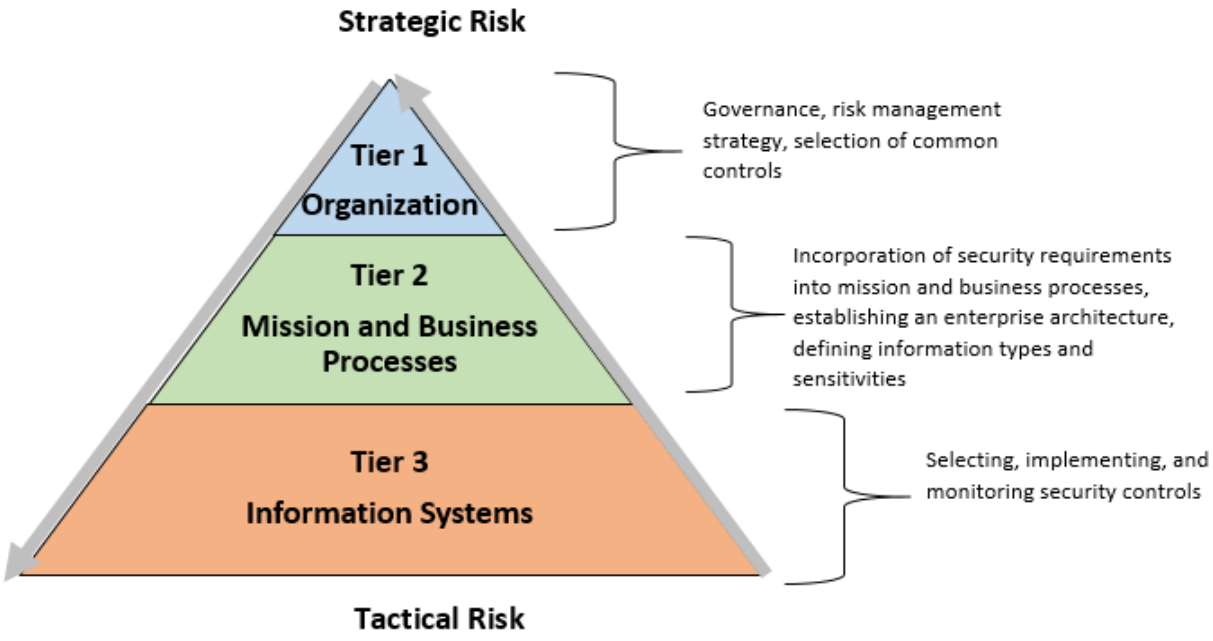
4. Office of Inspector General, *2014 Audit of the CFPB's Information Security Program,* OIG Report 2014-IT-C020, November 14, 2014.

Risk Management

Requirement

Risk management refers to the program and supporting processes used to manage information security risk to organizational operations, assets, individuals, and other organizations. This includes establishing the context for risk-related activities, assessing risk, responding to risks, and monitoring risks over time. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, notes that managing risk is a complex, multifaceted activity that requires the involvement of the entire organization. As depicted in figure 2 below, to best integrate the risk management process throughout an organization and more effectively address mission and business concerns, a three-tiered approach is employed that addresses risk at the organization, mission and business process, and information system levels.

Figure 2: The Three Tiers of Risk Management



Source: NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

One organization-level risk that has garnered considerable attention recently in the federal government is that of insider threats. Personnel who are entrusted with sensitive agency data can pose specific types of security risks to organizations, both intentionally and inadvertently. For example, trusted employees of the agency may feel justified in pursuing malicious activity against the organization, or they may be exploited by outside adversaries to inflict harm against the organization. These particular types of insider threats have become increasingly common and have been the source of several recent and highly publicized data breaches across the public and private sectors.

The importance of managing risks from insider threats led to the issuance of Executive Order 13587 as well as the *National Insider Threat Policy*. Executive Order 13587 directs executive agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect classified national security information. Although the CFPB has determined that these requirements do not apply to the agency because it does not handle classified information, NIST notes that the standards and guidelines can also be employed effectively to improve the security of controlled unclassified information in non–national security systems. [5] Technical components of such a program should include effective DLP solutions.

Progress to Date

In accordance with the three-tiered risk management approach defined by NIST, the CFPB has established a risk assessment methodology that is integrated at the organization, business process, and information system levels. This risk assessment methodology has been updated to consider both malicious and nonmalicious insider threats. Specifically, the CFPB has developed several risk monitoring reports and incident management practices that consider the risk of insider threats. Further, we noted that the CFPB's annual security awareness training includes content regarding malicious and nonmalicious insider threats, and agency officials informed us that the agency is prioritizing the implementation of a DLP program to complement its risk management and IR programs.

Work to Be Done

While the CFPB considers the threats that insiders pose as a part of its cybersecurity risk assessment methodology, the agency does not have an agency-wide insider threat strategy or program. Further, components of an effective insider threat program—including policies; implementation plans; and host-based user monitoring and DLP tools to deter, detect, and mitigate actions by employees who may represent a threat—have not been implemented. CFPB officials indicated that the agency's organizational structure and limited resources have affected its ability to effectively implement a centralized insider threat program. However, given the sensitive nature of the data collected by the CFPB to fulfill its mission, we believe that an agency-wide insider threat program that leverages existing IR capabilities can better inform and guide organizational risk management efforts and further protect the confidentiality, integrity, and availability of the agency's data.

5. NIST Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* defines *insider threat* as a threat that an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities.

Recommendation

We recommend that the Chief Information Officer (CIO), in coordination with the Chief Operating Officer

1. Evaluate options and develop an agency-wide insider threat program to include

    a. a strategy to raise organizational awareness.

    b. an optimal organizational structure.

    c. integration of IR capabilities, such as ongoing activities around DLP.

Management's Response

In his response to our report, the Acting CIO concurs with our recommendation. The Acting CIO indicates that the CFPB will coordinate across the agency to enhance its security education and training program to include more in-depth operational security facets of insider threats. Additionally, the Acting CIO states that the CFPB will institute new standards related to segregation of duties and other countermeasures that help manage insider threat risks. Lastly, the Acting CIO notes that the CFPB will leverage its DLP tools and incident response processes to assist in preventing and identifying the security events associated with insider threats.

OIG Comment

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

Identity and Access Management

Requirement

Effective identity and access management is a key control area for managing the risk from insider threats. Identity and access management includes implementing a set of capabilities to ensure that users authenticate to IT resources and have access to only those resources that are required for their job function, a concept referred to as *need to know*. FISMA requires agencies to implement controls to preserve authorized restrictions on access and disclosure. A key component of effective identity and access management is controlling the use of privileged accounts that possess elevated rights and are empowered with broad, direct access to information systems.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, emphasizes the importance of tracking and controlling the use of administrative privileges and ensuring that these privileges are periodically reviewed

and adjusted. This is further highlighted in the federal Cybersecurity Sprint,[6] which emphasizes the need for two-factor authentication through personal identity verification (PIV) cards or an assurance level 4 credential.[7]

CFPB's information security policies and procedures require that privileged users complete a user access form (UAF) to be approved by the appropriate manager or supervisor. Further, privileged users are required to sign rules of behavior (ROB) to ensure that they recognize, acknowledge, and adhere to the additional responsibilities of their special access to and privileges for computer resources supporting the agency. Violation of these rules could result in the loss of or limitations on the use of information resources as well as disciplinary or legal action, including but not limited to termination of employment or referral for criminal prosecution. Users who hold privileged access must annually resubmit their signed and approved UAFs and ROBs or their privileged access will be revoked.

Progress to Date

In August 2015, the CFPB completed migration of its IT infrastructure from the U.S. Department of the Treasury (Treasury). In May 2016, the CFPB updated its access control process document to reflect this transition. This document outlines the process for requesting, granting, and disabling privileged system access for privileged users. In addition, the agency has an ongoing project to manage identity and access credentials. As a part of this project, the CFPB has enabled PIV across its enterprise. Although PIV is not currently enforced, the agency has developed a project plan to deploy PIV credentials and resolve outstanding technical issues.

Work to Be Done

Several privileged users from our sample were either missing their signed UAF or ROB documentation or had not resubmitted their UAF or ROB documentation in the past year. Further, we found that access for users who had not resubmitted their UAF or ROB documentation within the past year had not been revoked. CFPB officials informed us that several of these privileged users identified as exceptions were granted access before the CFPB's transition from the Treasury infrastructure and had not been recertified.

By nature of their job function and level of access, insider threats from privileged users can pose a high level of risk to the CFPB's IT systems and sensitive information. We believe that by enforcing the agency's access control process, the CFPB can achieve greater assurance that personnel are maintaining their privileged access on a need-to-know basis. Further, by ensuring the maintenance of UAF and ROB documents for privileged users, the agency can have greater assurance that these users are fully aware of the rules and expected behavior they must abide by, as well as any resulting consequences of inappropriate behavior.

6. A 30-day Cybersecurity Sprint was launched by OMB in June 2015 to further improve federal cybersecurity and protect systems against these evolving threats.

7. OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003, defines four levels of assurance in terms of the consequences of authentication errors and the misuse of credentials. Level 1 is the lowest assurance level, and level 4 is the highest.

Recommendation

We recommend that the CIO

2. Ensure that

    a. a signed UAF and ROB document is on file and maintained for each privileged user.

    b. all privileged user accounts are annually recertified.

Management's Response

In his response to our report, the Acting CIO concurs with our recommendation and notes that the CFPB has commenced the deployment of information systems that specifically address the UAF and ROB processes. The Acting CIO also states that the CFPB will eliminate paper-based artifacts in favor of electronic records. These capabilities will automate workflows and centralize data regarding each privileged user and account. Further, the Acting CIO states that the CFPB is deploying automated solutions to ensure timely and accurate review and approval of the various forms of access that are used by privileged users, as well as the privileged accounts that support them in the performance of their duties.

OIG Comment

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

Contingency Planning

Requirement

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. FISMA requires agencies to develop, document, and implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (SP 800-34), provides best practices for information system contingency planning using a seven-step process. These seven steps are (1) developing contingency planning policy, (2) conducting a BIA, (3) identifying preventive controls, (4) developing recovery strategies, (5) developing the information system contingency plan, (6) testing the plan and training personnel, and (7) maintaining the plan.

NIST SP 800-34 also highlights the interrelationships between an information system contingency plan and other types of security and emergency management–related contingency plans that affect organizational resiliency. Specifically, an information system contingency plan provides established procedures for the assessment and recovery of a system following a

disruption. The plan may be activated independently or as part of a larger recovery effort in coordination with an agency's COOP, which is focused on restoring an organization's mission-essential functions. A key step in bringing these two contingency components together is the performance of a BIA. The purpose of the analysis is to correlate the system with the critical mission and business processes and services provided and, based on that information, characterize the consequences of a disruption. Results from the analysis should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP as well as the contingency planning requirements and priorities in the information system contingency plan.

Progress to Date

The CFPB released a contingency planning process document in September 2013. This document provides requirements and guidance for developing, testing, and maintaining contingency plans for the CFPB's systems as well as related training. We also found that the CFPB developed an agency-wide COOP, which was last approved in September 2015, as well as an information technology contingency plan (ITCP), which was released in June 2016, that contains system-specific contingency information. In addition, the CFPB maintains an offsite data processing facility, equipped with hardware and software, to be used in the event of an information system disruption. CFPB officials informed us that this offsite facility maintains backups of files and servers for restoration in the event of an outage or data loss.

Work to Be Done

We found that an agency-wide BIA has not yet been performed to guide the CFPB's contingency program, which includes the agency's ITCP and COOP. In addition, we found that that the agency's COOP is out of date, as it references recovery procedures for Treasury processes that have since been transitioned. Further, some of the information in the COOP is inconsistent with the recovery procedures documented in the CFPB's ITCP. For example, the COOP references Treasury's local area network disaster recovery site; however, the agency's ITCP states that the CFPB maintains its own alternate processing site for its IT infrastructure and in the event of a failure, this facility will serve as the alternate processing site for business continuity until the primary site is restored.

One reason for these contingency planning weaknesses is the timing of the agency's updates to its COOP and ITCP in relation to the agency's transition from the Treasury infrastructure. Specifically, we believe the COOP and ITCP inherited basic business impact information regarding its environment from the Treasury contingency program and have not been updated by the CFPB since the transition of its IT infrastructure. We believe that the performance of an agency-wide BIA that identifies critical mission and business processes, resource requirements, and system-level recovery priorities will inform both the COOP and ITCP and help the agency achieve a more effective contingency program.

Recommendation

We recommend that the CIO, in coordination with the Chief Operating Officer:

3. Strengthen the CFPB's contingency program by

    a. performing an agency-wide BIA.

    b. updating the agency's COOP and ITCP to reflect the results of the BIA and the current operating environment of the CFPB.

Management's Response

In his response to our report, the Acting CIO concurs with our recommendation. The Acting CIO indicates that in fiscal year (FY) 2017, the CFPB plans to include the collection of cross-functional information regarding the business impacts of various service-impacting events as identified via its new risk assessment methodology. The Acting CIO states that the CFPB will work closely with its internal partners who maintain and test the agency's COOP and who oversee its emergency management, personnel security, and physical security programs to modernize and harmonize these programs.

OIG Comment

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

Information Security Continuous Monitoring

Requirement

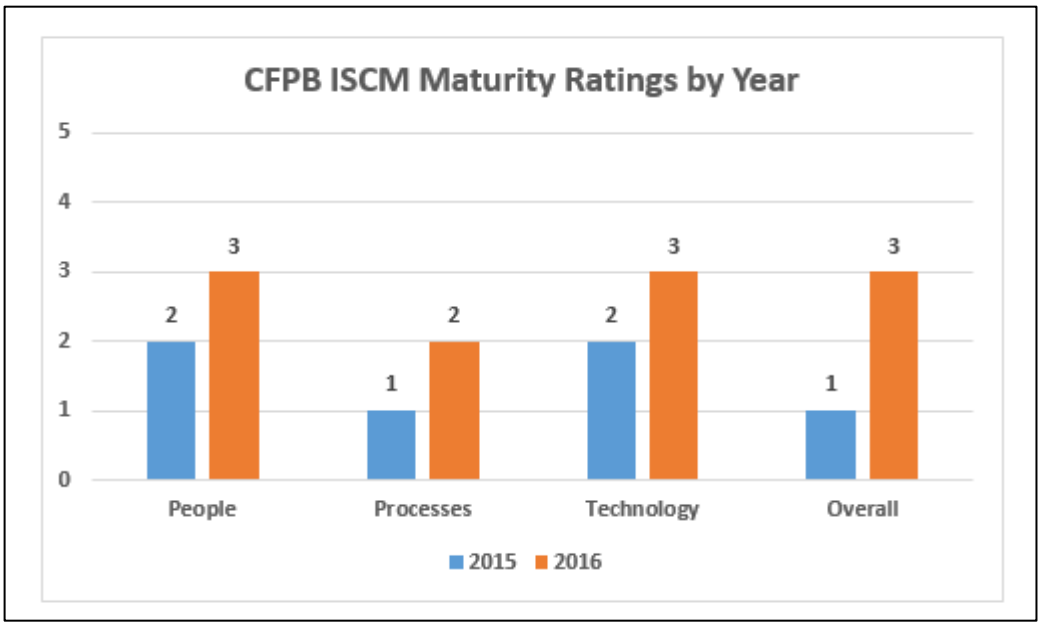
ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. FISMA emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a risk-based frequency. 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). Given the importance of ISCM in ensuring the security of federal information systems, OMB designated ISCM as a cybersecurity cross-agency priority for FY 2015 through FY 2017.

As previously noted, ISCM was the first domain chosen to be assessed under a maturity model approach in DHS's FISMA reporting guidance for IGs because it is a critical governmentwide focus area. ISCM was the first domain chosen to be assessed under a maturity model approach because of its critical role within an agency's information security program. As noted earlier, there are five levels of maturity, of which level 4 (*managed and measurable*) represents an effective program. As outlined in appendix B, DHS has provided a scoring methodology for IGs to determine the maturity of their agency's ISCM program.

Progress to Date and Work to Be Done

Last year, we found that that the CFPB's ISCM program was operating at level 1 (*ad hoc*), with the agency performing several, but not all, recommended activities indicative of higher maturity levels. For 2016, we determined that the agency has taken several steps to mature its ISCM program in accordance with NIST SP 800-137. As such, the CFPB's ISCM program was operating at level 3 (*consistently implemented*) (figure 3).

Figure 3: Maturity Levels for CFPB's ISCM Program (2015–2016)



Source: OIG analysis.

To reach level 4 (*managed and measurable*) and achieve an effective ISCM program, we identified several aspects within the people, processes, and technology domains that need to be strengthened. These include implementing alerting capabilities, adopting the Continuous Diagnostics and Mitigation (CDM) program, and establishing metrics to measure the effectiveness of the ISCM program. The following sections provide additional details on the maturity of the CFPB's ISCM program by domain, including steps we believe the agency should prioritize in the next year to better ensure the effectiveness of its ISCM program.[8]

People

As highlighted in figure 3 above, we found that the CFPB has matured its ISCM program in the people domain from level 2 (*defined*) to level 3 (*consistently implemented*). Specifically, roles and responsibilities have been fully defined and communicated across the organization, and

8. 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.

personnel performing ISCM functions have begun to receive training on the ISCM processes and tools utilized in the agency's environment. Further, the CFPB uses contractors, when necessary, to ensure adequate staffing, training, and resources to achieve the objectives of the agency's ISCM program. The CFPB continues to make progress in implementing its role-based security training program, which includes training for ISCM personnel on the processes performed throughout the agency. In conjunction with improvements noted below in the processes and technology domains, the CFPB can further mature its ISCM program by ensuring that skilled personnel are trained to develop and use appropriate security metrics to monitor the success of the program, once those metrics have been fully defined and implemented.

Processes

We found that the processes domain of the CFPB's ISCM program has improved from level 1 (*ad hoc*) to level 2 (*defined*), with several, but not all, ISCM processes performed in a manner indicative of a higher maturity level. Specifically, we found that the agency's processes for performing ongoing security control assessments, managing common vulnerabilities, reporting ISCM findings, and implementing risk responses are consistently implemented. Further, the CFPB has employed a formal lessons-learned process to facilitate ongoing improvements in the agency's ISCM program.

However, we also found two areas in the processes domain in which the CFPB can continue to mature its ISCM program. During our 2016 audit, we reviewed the actions taken by the agency to define, standardize, and automate its processes for hardware asset management. We found that the CFPB has developed a standard operating procedure to perform asset management functions and has begun to populate hardware assets into an automated solution for inventory tracking purposes. However, all assets have not yet been cataloged in this tool. CFPB officials informed us that the agency is planning to implement additional asset management tools as part of DHS's CDM program. We believe that the agency should continue to mature its own asset management process and work toward the implementation of the CDM program in order to implement an effective hardware asset management function.

Further, we found that the CFPB is currently collecting data, tracking, and reporting quarterly on three ISCM-related security metrics in the areas of people, processes, and technology. As the agency continues to utilize its suite of tools to manage organizational security, we believe that the use of additional qualitative and quantitative security metrics to measure the effectiveness of ISCM processes will provide further insight into the effectiveness of the agency's ISCM program.

Technology

We found that the technology domain of the CFPB's ISCM program has improved from level 2 (*defined*) to level 3 (*consistently implemented*), with a suite of tools consistently implemented to cover most of the automation areas outlined in NIST SP 800-137.[9] Further, the CFPB has

9. 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.

implemented an automated solution to produce an accurate point-in-time inventory of the devices, as well as the security configurations of those devices, on its network.

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 agency had identified the tools it planned to implement in these areas.[10] This year, we noted that these tools had been consistently implemented. As such, we believe that the CFPB has taken sufficient actions to close this recommendation.

We did identify areas within the technology domain of the agency's ISCM program, however, that should be prioritized to help ensure an effective ISCM program. For instance, although the CFPB has implemented a number of tools to mature its ISCM program, the agency is still customizing a solution that will enable it to centralize and further automate its ISCM reporting and dashboard capabilities. We will continue to monitor the agency's progress in implementing this solution as a part of our future FISMA audits.

We also found that the agency is continuing to mature its technological solutions in the areas of asset management, as detailed above, and license management through DHS's CDM program. The CFPB has been placed within Group F, a collection of smaller agencies and the last of the six groups scheduled for implementation of procured CDM capabilities. The agency is working to build out and automate these particular aspects of its ISCM program as it prepares for the CDM tools and services to complement and strengthen the agency's program. As the CFPB continues to mature, the agency may also want to consider other aspects of its program where it can leverage additional capabilities and tools, such as configuration setting and vulnerability management, which are a part of the CDM program specifically designed to protect privacy data and fulfill FISMA mandates.

The CFPB has taken a number of steps in 2016 to mature its ISCM program. We will continue to monitor the agency's progress to develop and implement an effective ISCM program as part of our future FISMA reviews.

Incident Response

Requirement

Several of the outputs of an effective ISCM program can provide key indicators of an agency's ability to detect, prevent, and respond to computer security incidents in a timely manner. As computer security incidents affecting the federal government have continued to increase in number and impact, implementing an effective IR capability has become a critical component of agency information security programs. FISMA requires agencies to develop and implement procedures for detecting, reporting, and responding to security incidents, including mitigating the risks of such incidents before substantial damage is done. In addition, FISMA requires agencies to notify and consult with the United States Computer Emergency Readiness Team (US-CERT). Specifically, agencies are required to notify US-CERT of all computer security

10. Office of Inspector General, *2015 Audit of the CFPB's Information Security Program,* OIG Report 2015-IT-C-020, November 13, 2015.

incidents involving a federal government information system with a confirmed impact to confidentiality, integrity, or availability within one hour.

Best practices for implementing an effective incident handling capability are outlined in NIST Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide* (SP 800-61). SP 800-61 highlights the important role that automation plays in incident detection and analysis, particularly with respect to analyzing the voluminous signs of incidents that can occur daily in an organization. As noted earlier in our report, there has been a renewed focus on managing insider threat risks across the government. An automated technology that could help detect insider threat actions and prevent both intentional and inadvertent data leaks is a DLP solution. SP 800-61 also 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 and mitigating any risks before substantial damage is done.

Progress to Date and Work to Be Done

We found that the CFPB's IR program is operating at level 3 (*consistently implemented*). However, we identified several opportunities to mature the agency's IR program in the areas of people, processes, and technology in order to ensure that the program is effective. The following sections provide additional details on the maturity of the CFPB's IR program by the people, processes, and technology domains, including the steps we believe that the agency should prioritize in the next year to develop an effective IR program.

People

We found that the people domain of the CFPB's IR program is operating at level 3 (*consistently implemented*), with IR roles and responsibilities fully defined and communicated across the organization. For example, the agency has implemented standard operating procedures for its Computer Security Incident Response Team, which includes responsibilities to coordinate and advise appropriate entities on the continuity and protection of normal operating conditions for information systems both before and after the occurrence of an adverse event. Further, we found that the CFPB utilizes the common threat vector taxonomy defined by US-CERT within its incident tracking tool. In conjunction with improvements noted below in the processes and technology domains, the CFPB can further mature its IR program by ensuring that skilled personnel are trained to develop and use appropriate security metrics to monitor the success and effectiveness of the program, once such metrics are fully defined and consistently implemented.

Processes

We found that the processes domain of the CFPB's IR program is operating at level 2 (*defined*), with several, but not all, processes performed at level 3 (*consistently implemented*) maturity. For example, we found that the CFPB is collecting and analyzing incident data from a number of sources to protect the agency's network. We also found that the agency documents incident detection, containment, and recovery activities consistently. Further, our 2013 FISMA report included a recommendation for the CFPB to ensure that audit logs and security incident

information from all relevant sources are centrally tracked, analyzed, and correlated.[11] This year, we noted that the agency has implemented an automated solution to perform these functions and, as detailed in the section below on the status of prior years' findings, we are closing this recommendation. We also found that the CFPB has implemented a formal lessons-learned process to facilitate ongoing improvements in the agency's IR program.

We identified several areas within the processes domain, however, in which the CFPB can mature its IR program to ensure that it is effective. Such areas include processes for reporting security incidents in a timely manner and collecting IR-related security metrics to measure the effectiveness of the program. Given the consequences that security breaches can have on the confidentiality, integrity, and availability of agency data, timely reporting is critical to an effective IR function. Coupled with the consistent analysis and documentation of IR activities already performed by the agency, we believe that timely reporting will further mature the effectiveness of the CFPB's IR program.

In addition, we found that the CFPB's incident tracking solution is capturing useful input data, such as incident source and response times, to measure the effectiveness of the agency's IR processes. CFPB officials informed us, however, that additional metrics for the IR program are still being built out as the new suite of tools is implemented throughout the agency. As the CFPB continues to use these tools to manage security, additional qualitative and quantitative security metrics to measure the effectiveness of incident response processes will provide further insight into the effectiveness of the agency's IR program.

Technology

We found that the technology domain of the CFPB's IR program is operating at level 2 (*defined*), with several processes performed in a manner indicative of a higher maturity level. Specifically, we found that since its transition from the Treasury infrastructure, the CFPB has contracted with a service provider to implement OMB's Trusted Internet Connections Initiative, which manages all agency traffic through defined access points.[12] Participation in the initiative is necessary to ensure all external connections are monitored by DHS's intrusion detection sensors, operationally known as the EINSTEIN program.[13] In addition, we found that the CFPB conducts periodic tests with DHS to ensure that these intrusion detection and prevention capabilities are operating as intended.

We identified opportunities, however, for the CFPB to mature its IR program through further automation by implementing a DLP solution. As noted above, a DLP solution is an important technical component of an effective risk management and insider threat program. CFPB officials informed us that as part of a defense-in-depth approach, the agency is prioritizing the implementation of a DLP program for its internal network. CFPB officials also noted that the

11. Office of Inspector General, *2013 Audit of the CFPB's Information Security Program,* OIG Report 2013-IT-C-020, December 2, 2013.

12. The purpose of the Trusted Internet Connections Initiative, as outlined in OMB Memorandum M-08-05, is to optimize and standardize the security of individual external network connections currently in use by federal agencies, including connections to the Internet.

13. EINSTEIN is an intrusion detection system, provided by DHS, to detect and block cyberattacks from compromising federal agencies and to provide situational awareness by using threat information detected in one agency to protect the rest of the government.

agency is taking a holistic and multipronged approach to DLP with the intent of implementing a program that will include policies and procedures, a DLP solution, and user training.

Status of Prior Years' Recommendations

As part of our annual FISMA audit, we reviewed the actions taken by the CFPB to address outstanding recommendations from our prior years' FISMA reviews. Below is a summary of the status of the recommendations that were open at the start of our 2016 FISMA audit. Based on corrective actions taken by the CFPB, we are closing six prior recommendations related to configuration management, security training, IR, policies and procedures, and remote access. One recommendation in the area of configuration management will remain open at this time. We will update the status of these recommendations in our upcoming *Semiannual Report to Congress* and continue to monitor the CFPB's progress in addressing the one open recommendation as a part of future FISMA reviews.

Information Security Continuous Monitoring

In our 2014 FISMA audit, we recommended that the CIO fully implement the CFPB'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 agency had identified the tools it planned to implement in these areas. This year, we noted that these tools had been consistently implemented. As such, we believe that the CFPB has taken sufficient actions to close this recommendation. The agency is still customizing a solution that will enable it to centralize and further automate its ISCM reporting and dashboard capabilities; therefore, we will continue to monitor the agency's progress in implementing this solution as a part of our future FISMA audits.

Configuration Management

In our 2013 FISMA report, we recommended that the CIO develop and implement an agency-wide configuration management plan and a consistent process for patch management. During our follow-up work in 2014 and 2015, we found that although the agency had implemented a patch management process consistent with FISMA and NIST requirements, it was working on developing a configuration management plan. This year, we found that the agency finalized its agency-wide configuration management plan. We reviewed the plan and found that it describes how configuration management policies will be implemented throughout the agency and includes the components recommended by NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*. As such, we conclude that the CFPB has taken sufficient actions to address this recommendation.

Our 2014 FISMA report also included a recommendation for the CIO to 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 2015, the agency was working to evaluate its current scanning solutions to determine whether the capacity to perform these types of scans could be leveraged from tools already implemented within their environment. In 2016, however, agency officials informed us that application and

database-level scanning will require the implementation of tools from the CDM program. As such, this recommendation will remain open, and we will continue to monitor CFPB's progress in this area as part of our future audit activities.

Security Training

In our 2013 FISMA report, we recommended that the CIO design, develop, and implement a role-based security training program for individuals with significant security responsibilities. In the intervening years, we found that the CFPB was working to develop and implement a role-based training process with content specific to the agency's environment. This year, we found that the agency has developed and implemented a role-based training program for users deemed to have significant security responsibilities. Specifically, the agency has developed knowledge units for specific groups of users and is continuing to refine training content to further mature the effectiveness of its security training program. Therefore, we conclude that the CFPB has taken sufficient actions to close this recommendation.

Incident Response

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. Since that time, the CFPB has procured a solution to provide this functionality and has developed a project plan to begin populating the tool with relevant incident information. As part of our 2016 FISMA testing, we found that the CFPB has made significant progress in implementing this functionality. Specifically, the agency has implemented the automated solution to collect audit log and security incident information for analysis and correlation. Most high-priority audit logs have been loaded into the tool, which is already in production and integrated into the agency's IR function. Although the CFPB is still refining the tool's alerting capabilities, we conclude that the agency has taken sufficient actions to close this recommendation.

Policies and Procedures

In our 2015 FISMA report, we recommended that the CIO 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. During our 2016 FISMA testing, we found that the majority of the agency's policy, procedure, and process documents had been revised to reflect the agency's current operating environment. For those security-related documents that had not yet been updated, we found that these items were currently going through the review and publication process. As such, we conclude that sufficient actions have been taken to close this recommendation.

Remote Access

In our 2015 FISMA report, we recommended that the CIO strengthen the cryptographic mechanism employed for the CFPB's remote access solution in accordance with NIST guidance. As a part of our 2016 FISMA testing, we found that the encryption mechanism used

for remote access to the agency's IT infrastructure has been updated to meet NIST standards. As such, we conclude that sufficient actions have been taken to close this recommendation.

Appendix A
Scope and Methodology

Our specific audit objectives, based on the requirements FISMA, were to evaluate the effectiveness of the CFPB's (1) security controls and techniques and (2) information security policies, procedures, and practices. To accomplish our objectives, we reviewed the effectiveness of the CFPB's information security program across the eight areas outlined in DHS's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. These areas are ISCM, configuration management, identity and access management, IR, risk management, security and privacy training, 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 network and operating system levels on select IT devices. We used the results of our review of the CFPB's information security program and testing of controls for an agency system to evaluate the implementation of specific attributes outlined in DHS's 2016 FISMA reporting guidance for IGs.

We performed our fieldwork from June 2016 to September 2016. 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
FISMA Scoring Methodology

This appendix contains the scoring methodology contained in DHS's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. IGs are required to use this methodology to determine the maturity level of their respective agency's information security programs. Specifically, based on the IGs' assessments, agencies are allotted points for each cybersecurity framework function area based on their achievement of various levels of maturity. For each framework function, a total of 20 points is possible. Last year, when determining the overall maturity for an agency's program, a lowest common denominator approach was used, meaning an agency could only meet a particular level of maturity if they met all ISCM security metrics defined for that level. The FY 2016 IG FISMA reporting metrics continue the effort begun in 2015; however, the lowest common denominator scoring approach has been removed. The scoring methodology for each maturity level is provided in table B-1 below.

Table B-1: Maturity Level Scoring Methodology

Maturity level	Scoring description	Scoring distribution
Level 1: *ad hoc*	Automatically receives points regardless of achievements.	3 points
Level 2: *defined*	For the identify, protect, and recover function areas, met at least half the metrics designated at level 2 (*defined*). For the detect and respond function areas, met all metrics designated at level 1 (*ad hoc*) and at least half those designated at level 2 (*defined*).	4 points
Level 3: *consistently implemented*	For all function areas, met all metrics designated at level 2 (*defined*) and at least half those designated at level 3 (*consistently implemented*).	6 points
Level 4: *managed and measurable*	For all function areas, met all metrics designated at level 3 (*consistently implemented*) and at least half those designated at level 4 (*managed and measurable*).	5 points
Level 5: *optimized*	For all function areas, met all metrics designated at level 4 (*managed and measurable*) and level 5 (*optimized*).	2 points

Source: OIG analysis of DHS's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

Appendix C
Management's Response

1700 G Street NW, Washington, DC 20552

November 4, 2016

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 *2016 Audit of the CFPB's Information Security Program.*

The Bureau is pleased to note that you record us as consistent with seven of the eight FY 2016 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Metric Domains--specifically Risk Management, Contractor Systems, Configuration Management, Identity and Access Management, Security and Privacy Training, Information Security Continuous Monitoring (ISCM), and Incident Response. During the next fiscal year, we will continue to improve and mature our processes and activities in the remaining contingency planning domain.

We are pleased that you found that the Bureau continues to mature our FISMA compliance and information security posture. The report noted our new risk assessment methodology that is integrated at the organization, business process, and information system levels, and how the methodology is tailored to ensure that the Bureau addresses insider as well as outsider threats, both malicious and non-malicious.

As your report points out, following the completion of our independence project, we refined and updated numerous process and standards publications, including our access control doctrine. Our Identity, Credential, and Access Management (ICAM) team is making great strides in automating our identity and authorization processes, for all levels of users across a broad spectrum of privileges and capabilities. In FY 2017, we will continue our personal identity verification (PIV) enablement and integration efforts, as well as automating the tracking of user permissions and associated agreements with behavior rules and usage policies.

Your report notes our continued work on contingency planning materials, with our new Information Technology Contingency Plan (ITCP). With the associated training and testing, we will enhance the effectiveness of our off-site backup facilities which, as you noted, are equipped with the necessary hardware, software, and data to support our information systems through a service-impacting event. These system-specific plans respond to risk management processes and decisions at the enterprise, business/mission, and IT levels, per National Institute of Standards and Technology (NIST) guidance, and support the agency-wide continuity of operations plan (COOP). In FY 2017, we will continue that work as we tune and harmonize the technological, operational, and managerial aspects of our contingency planning work. This work will focus on business-driven impact factors such as time-sensitivity and resiliency, as experienced by the various business units that drive the requirements behind our technology programs. Through analyses of such business impact information, we will continue to take steps to mature our capabilities in this FISMA domain.

We are pleased that you have found that our ISCM program has matured from level one to level three, as defined by the ISCM maturity model included in the FY2015 FISMA reporting guidance. When comparing our rating for this year to the rating of the CFO Act Agencies and Small Agencies who were scored using the ISCM maturity model last year (as documented in OMB's *Annual Report to Congress: Federal Information Security Modernization Act*), CFPB has out-performed 91.7% of the CFO Act Agencies and 76.3% of the Small Agencies. We view this as an attestation of the significant work we have applied in the ISCM domain, where we captured "lessons learned" that informed our prioritization and resource allocation decisions, thus allowing us to hone and improve our ISCM program, and jump from level one to level three within the course of a single fiscal year. We will use your feedback regarding ISCM metrics and measurements to help move the Bureau towards a level four "Managed and Measurable" rating during the course of FY 2017.

This year, your report notes that the maturity of our Incident Response domain has been measured at level three as defined in the FISMA reporting guidance. The deployment of our new Security Event and Incident Management (SEIM) platform is already providing us with valuable information that enhances the timeliness and responsiveness of our existing procedures, which we crafted in agreement with NIST guidance. We look forward to leveraging our SEIM in conjunction with other improvements in our processes as we move toward the fourth level of maturation. We will also enhance our user education and incident response procedures to ensure that reporting times to the United States Computer Emergency Readiness Team (US-CERT) and other parties are at optimum, risk-based levels.

We appreciate your noting our progress on remediating recommendations from previous Inspector General (IG) reviews. We value your objective, independent viewpoints and consider our IG to be a trusted source of informed, accurate, and insightful information. This year, you reported upon the success of our efforts to address many of the valuable recommendations that you have provided to us in the past. We are pleased that you consider six of the seven recommendations that existed at the start of this year's FISMA audit to have been successfully closed through our remediation efforts. We will also be working to ensure that the areas of application and database security configurations are successfully addressed once DHS concludes their deployment of the Continuous Diagnostics and Mitigation (CDM) solution in our infrastructure.

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

Sincerely,

VIJAY DESAI Digitally signed by VIJAY DESAI
Date: 2016.11.04 10:21:39
-04'00'

Vijay Desai
Chief Information Officer (Acting)

consumerfinance.gov

Response to recommendations presented in the Draft IG Report, "*2016 Audit of the CFPB's Information Security Program*."

Recommendation 1: Evaluate options and develop an agency-wide insider threat program to include *(a)* a strategy to raise organizational awareness; *(b)* an optimal organizational structure; and *(c)* integrated IR capabilities, such as ongoing activities around DLP.

Management Response: The Bureau concurs with this recommendation. The Bureau is well informed on Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and the resulting insider threat security control requirements as articulated by National Institute of Standards and Technology (NIST). We will be coordinating across the Bureau to enhance our security education and training program to include more in-depth operational security facets of the insider threat. We will also be instituting new standards related to segregation of duties and other countermeasures that work to help manage the insider threat risk. Further, we will be leveraging our Data Loss Prevention (DLP) tools and incident response processes to assist in preventing and identifying the security events associated with insider threats. There is no single countermeasure to insider threats, and our approach will continue to grow as a balanced, risk-reasoned stance that bridges technological aspects with people and well-defined processes.

Recommendation 2: Ensure that (a) a signed UAF and ROB document is on file and maintained for each privileged user and (b) all privileged user accounts are annually recertified.

Management Response: The Bureau concurs with this recommendation. Even prior to the issuance of your report, the Bureau had commenced deployment of information systems that specifically address the User Access Forms (UAF) and Rules of Behavior (ROB) processes. We are eliminating paper-based artifacts in favor of electronic records. These capabilities will automate workflows and centralize data-of-record regarding each privileged user and each privileged account. Further, we are deploying automated solutions to ensure timely and accurate review and approval of the various forms of access that are used by our privileged users, as well as the privileged accounts that support them in the performance of their duties.

Recommendation 3: Strengthen the CFPB's contingency program by (a) performing an agency-wide BIA and (b) updating the agency's COOP and IT contingency plan to reflect the results of the BIA and the current operating environment of the CFPB.

Management Response: The Bureau concurs with this recommendation. In FY 2017, our plans include the collection of cross-functional information regarding the business impacts of various service-impacting events as identified via our new risk assessment methodology, and mapped to

the various artifacts that describe our responses to these events. We will be working closely with our internal partners who maintain and test the Bureau's Continuity of Operations Plan (COOP), as well as oversee our emergency management, personnel security, and physical security programs to modernize and harmonize these programs. This will, among other benefits, enhance our COOP, our Information Technology Contingency Plan (ITCP) program, and other related business processes.

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