Audit Report
2018-IT-C-018
October 31, 2018

Bureau of Consumer Financial Protection

2018 Audit of the Bureau's Information Security Program

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Executive Summary, 2018-IT-C-018, October 31, 2018

2018 Audit of the Bureau's Information Security Program

Findings

The Bureau of Consumer Financial Protection's (Bureau) information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. For instance, the Bureau's information security continuous monitoring process is effective and operating at level 4 (*managed and measurable*), with the agency reporting on performance measures related to supporting activities. Further, the Bureau's incident response process is similarly effective, with the agency using tools to detect and analyze incidents and track performance metrics.

The Bureau also has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five Cybersecurity Framework security functions—*identify, protect, detect, respond,* and *recover*—to ensure that its program is effective. Specifically, as we noted last year, the agency can strengthen its enterprise risk management program by defining a risk appetite statement and associated risk tolerance levels. The Bureau can also improve its processes related to database security, timely remediation of vulnerabilities, and patching of mobile phone operating systems. Further, access to one of the Bureau's internal collaboration tools, which contains sensitive information (including personally identifiable information), was not restricted to individuals with a need to know.

Finally, the Bureau has taken sufficient action to close 3 of the 10 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to identity and access management, incident response, and contingency planning. We will continue to monitor the Bureau's progress as part of future FISMA reviews.

Recommendations

This report includes 4 new recommendations designed to strengthen the Bureau's information security program in the areas of configuration management, identity and access management, and data protection and privacy. In response to a draft of our report, the Chief Information Officer concurs with our recommendations and outlines actions that have been or will be taken to address them. We will continue to monitor the Bureau's progress in addressing these recommendations as part of future audits.

Purpose

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

Background

FISMA requires each Inspector General to conduct an annual independent evaluation of its agency's information security program, practices, and controls for select systems. U.S. Department of Homeland Security guidance for FISMA reporting directs Inspectors General to evaluate the maturity level (from a low of 1 to a high of 5) of their agency's information security program across several areas. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.

Recommendations, 2018-IT-C-018, October 31, 2018

2018 Audit of the Bureau's Information Security Program

Number	Recommendation	Responsible office
1	Strengthen configuration management processes by a. remediating configuration-related vulnerabilities in a timely manner. b. ensuring that optimal resources are allocated to perform vulnerability remediation activities.	Office of Technology and Innovation
2	Develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.	Office of Technology and Innovation
3	Determine whether established processes and procedures for management of user-access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.	Office of Technology and Innovation
4	Ensure that the Bureau's existing information security continuous monitoring approach is implemented for an internal collaboration tool to appropriately restrict and monitor access.	Office of Technology and Innovation

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

MEMORANDUM

DATE: October 31, 2018

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2018-IT-C-018: *2018 Audit of the Bureau's Information Security Program*

We have completed our 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 select security controls for cloud-based systems as part of our ongoing evaluation of the Bureau's processes for leveraging the Federal Risk and Authorization Management Program. The detailed results of that review will be transmitted under a 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 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

We provided you with a draft of our report for your review and comment. In your response, you concur with our recommendations and state that actions have been or will be taken to address them. We have included your response as appendix B to our report.

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

cc: Claire Stapleton, Chief Privacy Officer
Michael (Scott) Braus, Acting Chief Information Security Officer, Division of Technology and Innovation
Katherine Sickbert, Deputy Chief Information Officer, Division of Technology and Innovation
Elizabeth Reilly, Chief Financial Officer and Assistant Director, Office of the Chief Financial Officer
Dana James, Deputy Chief Financial Officer, Office of the Chief Financial Officer
Anya Veledar, Finance and Policy Analyst, Office of the Chief Financial Officer
Carlos Villa, Finance and Policy Analyst, Office of the Chief Financial Officer

Distribution:
Jerry Horton, Chief Information Officer
Katherine Fulton, Acting Chief Operating Officer and Deputy Chief of Staff
Marianne Roth, Chief Risk Officer

Contents

Introduction

Objectives

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

Background

FISMA requires agencies to develop, document, and implement an agencywide security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or another source.[1] FISMA also requires that each 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.

To support annual independent evaluation requirements, the U.S. Department of Homeland Security (DHS) publishes FISMA reporting metrics for IGs to respond to on an annual basis. This guidance directs IGs to evaluate the effectiveness of agency information security programs across a variety of attributes grouped into eight security domains. These domains align with the five security functions defined by the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) (table 1).[2]

[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] The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

Table 1. Cybersecurity Framework Security Functions, Objectives, and Associated FISMA IG Reporting Domains

Security function	Security function objective	Associated FISMA IG reporting domain
Identify	Develop an organizational understanding to manage cybersecurity risk to agency assets	Risk management
Protect	Implement safeguards to ensure delivery of critical infrastructure services as well as prevent, limit, or contain the impact of a cybersecurity event	Configuration management, identity and access management, data protection and privacy,[a] and security training
Detect	Implement activities to identify the occurrence of cybersecurity events	Information security continuous monitoring
Respond	Implement processes to take action regarding a detected cybersecurity event	Incident response
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event	Contingency planning

Source. U.S. Department of Homeland Security, *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

a. The data protection and privacy domain was added to the annual IG FISMA reporting metrics in 2018. This domain includes metrics for assessing the effectiveness of the agency's privacy program, security controls to protect personally identifiable information, enhanced network defenses, responses to data breaches, and privacy awareness training.

FISMA Maturity Model

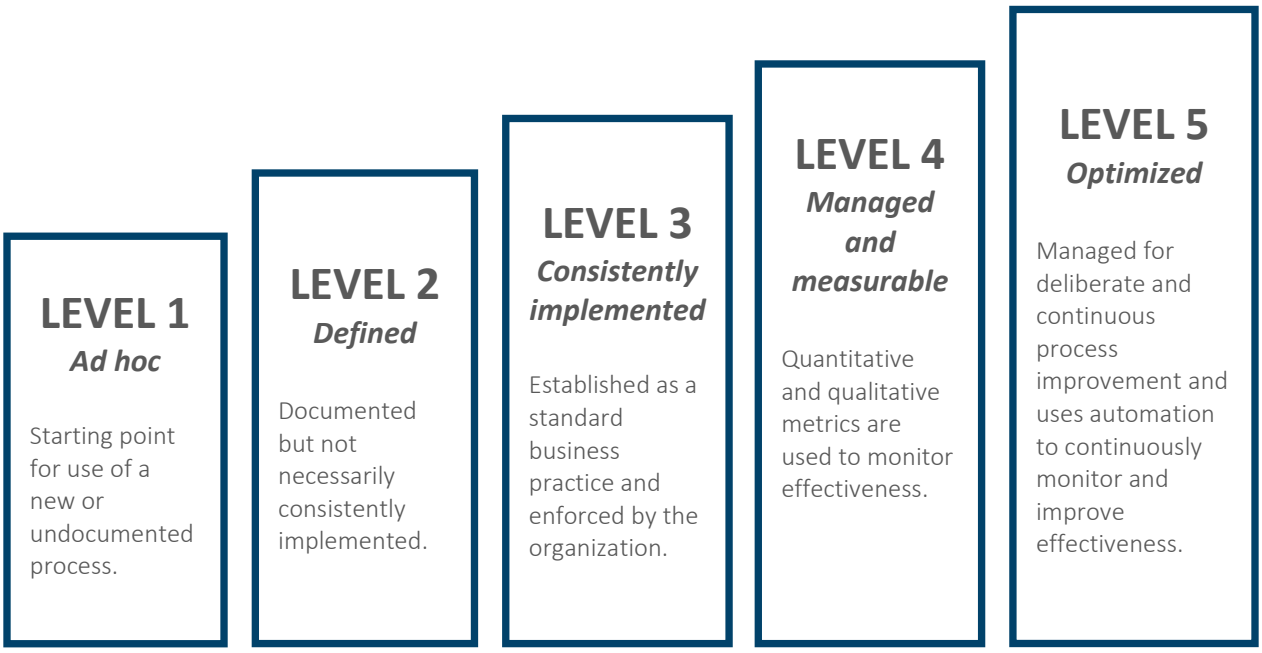
FISMA requires that IGs assess the effectiveness of information security controls that support the operations and assets of their respective agency. To that end, the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Office of Management and Budget (OMB), DHS, and other key stakeholders, developed a maturity model intended to better address and report on the effectiveness of an agency's information security program. The purpose of the maturity model is to (1) summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) provide transparency to agency Chief Information Officers (CIOs), 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) help ensure that annual FISMA reviews are consistent across IGs.

The five levels of the IG FISMA maturity model are

1. *ad hoc*
2. *defined*
3. *consistently implemented*
4. *managed and measurable*
5. *optimized*

The foundational levels (1–3) of the model are geared toward the development and implementation of policies and procedures, and the advanced levels (4–5) capture the extent to which agencies institutionalize those policies and procedures (figure 1). The maturity levels of each of the security domains will dictate the overall maturity of an organization's information security program. As noted in DHS's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* level 4 (*managed and measurable*) represents an effective level of security.[3] This is the second year that all FISMA security domains will be assessed using a maturity model. Details on the scoring methodology for the maturity model can be found in appendix A.

Figure 1. FISMA Maturity Model Rating Scale



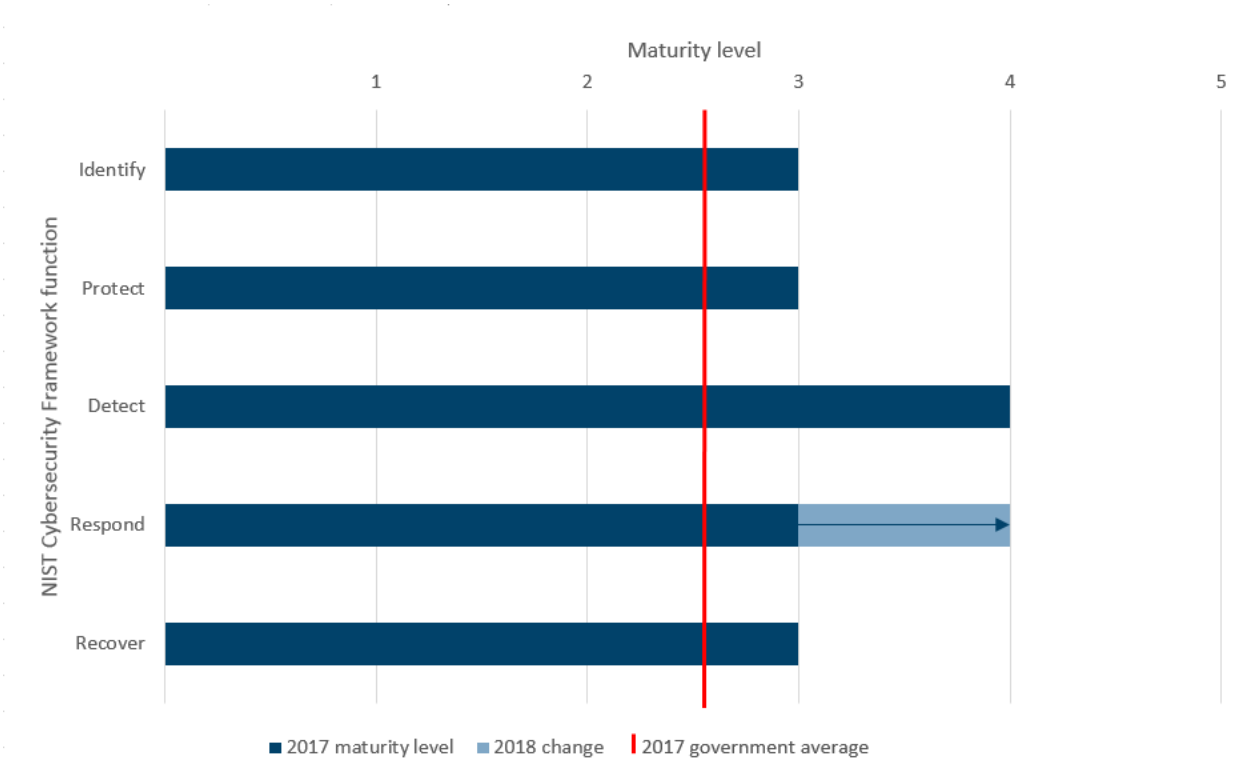
Source. OIG analysis of DHS IG FISMA reporting metrics.

[3] NIST Special Publication 800-53, Revision 4, *Security and Privacy of Controls for Federal Information Systems and Organizations*, defines security control effectiveness as 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, or enforcing or mediating established security policies.

Summary of Findings

The Bureau's overall information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level (figure 2).[4] For instance, the Bureau's information security continuous monitoring (ISCM) process is effective and operating at level 4, with the agency tracking and reporting on performance measures related to supporting activities. Further, the Bureau's incident response process is effective and operating at level 4, with the agency using multiple tools to detect and analyze incidents and track performance metrics.

Figure 2. Maturity of the Bureau's Information Security Program



Source. OIG analysis.

As highlighted in table 2, the Bureau has further opportunities to ensure that its information security program is effective in FISMA domains across all five Cybersecurity Framework security functions: *identify, protect, detect, respond,* and *recover*. Our report includes four new recommendations in the *protect* function area as well as several items for management's consideration.

[4] Appendix A of this report explains the scoring methodology used to determine the maturity of the Bureau's information security program.

Table 2. Summary of Opportunities to Mature the Bureau's Information Security Program

Cybersecurity function area and IG FISMA reporting domain	Maturity rating	Opportunities for improvement
Identify		
Risk management	Level 3: *consistently implemented*	• Develop and implement an agencywide risk appetite statement and risk tolerance levels (2017 recommendation).
Protect		
Configuration management	Level 3: *consistently implemented*	• Remediate configuration-related vulnerabilities in a timely manner (2018 recommendation). • Ensure that patches and security updates are applied timely for the agency's mobile phones (2018 recommendation).
Identity and access management	Level 3: *consistently implemented*	• Ensure that processes for managing access agreements and rules of behavior for individuals with privileged access to Bureau systems are effective and adequately resourced (2018 recommendation).
Data protection and privacy	Level 3: *consistently implemented*	• Ensure that the Bureau's existing ISCM approach is implemented for an internal collaboration tool to appropriately restrict and monitor access. (2018 recommendation). • Deploy data loss prevention tool across the agency.
Security training	Level 3: *consistently implemented*	• Deploy the phishing exercise program across all divisions to measure the effectiveness of security awareness and training activities (2017 recommendation).
Detect		
Information security continuous monitoring	Level 4: *managed and measurable*	• Strengthen monitoring of security configurations for databases and applications through greater automation (2014 recommendation). • Incorporate technologies and processes provided through the DHS continuous diagnostics and mitigation program when they are made available.
Respond		
Incident response	Level 4: *managed and measurable*	• Ensure applicable alerts and logs from applications residing in the Bureau's new cloud computing environment are uploaded to the agency's central automated solution (2017 recommendation).
Recover		
Contingency planning	Level 3: *consistently implemented*	• Perform an agencywide business impact analysis (2016 recommendation). • Ensure that the results of contingency testing are leveraged to make risk-based decisions at an enterprise level. • Integrate contingency plan development and maintenance with other continuity areas such as the insider threat plan and the occupant emergency plan.

Source. OIG analysis.

In addition, the Bureau has taken sufficient action to close 3 of the 10 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to identity and access management, incident response, and contingency planning. We are leaving open 7 recommendations in the areas of risk management, configuration management, identity and access management, security training, incident response, and contingency planning from our 2014, 2016, and 2017 FISMA audits.[5] We will continue to monitor the Bureau's progress in addressing these open recommendations as part of future FISMA audits. The disposition of these recommendations is detailed in the Status of Prior Years' Recommendations section of this report.

[5] Office of Inspector General, *2014 Audit of the CFPB's Information Security Program*, OIG Report 2014-IT-C-020, November 14, 2014; Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*, OIG Report 2016-IT-C-012, November 10, 2016; Office of Inspector General, *2017 Audit of the CFPB's Information Security Program*, OIG Report 2017-IT-C-019, October 31, 2017.

Analysis of the Bureau's Progress in Implementing Key FISMA Information Security Program Requirements

The Bureau's overall information security program is operating at a level-3 (*consistently implemented*) maturity. Although the agency has strengthened its program since our 2017 FISMA review, it has further opportunities to ensure that its information security program is effective across specific FISMA domains in all five Cybersecurity Framework security functions: *identify, protect, detect, respond,* and *recover*.

Identify

The objective of the *identify* function in the Cybersecurity Framework is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities. The Cybersecurity Framework highlights risk management processes that organizations can implement to inform and prioritize decisions.

Risk Management

FISMA requires federal agencies to provide information security protections commensurate with their risk environment. Risk management refers to the program and supporting processes used to manage risk to organizational operations, assets, and individuals. This includes establishing the context for risk-related activities, assessing risks, responding to risks, and monitoring risks over time. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (SP 800-39), states that managing risk is a complex, multifaceted activity that requires the involvement of the entire organization. To accomplish this, risk management must be addressed at the enterprise, mission and business process, and information system levels.

Enterprise risk management (ERM) is an area that has seen increased emphasis in the federal government. It refers to an effective agencywide approach to addressing the full spectrum of the agency's external and internal risks. OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, provides guidance for implementing an ERM capability and governance structure that is coordinated with strategic planning and internal control processes.[6]

As part of the ERM governance structure, OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires that agencies designate a senior accountable official for risk management. This official is responsible for (1) ensuring that risk management processes are aligned with strategic, operational, and budgetary planning processes and (2) reporting to DHS and OMB on risk management decisions and the agency's plan to implement the NIST Cybersecurity Framework. In addition to a governance structure, the

[6] Although OMB Circular A-123 is not directly applicable to the Bureau, other agencies, such as nonexecutive agencies, are encouraged to adopt the circular.

development of an agencywide risk context is a key component of ERM. Other key components of ERM include defining risk appetite and risk tolerance levels, a risk management strategy, and a risk profile (table 3).

Table 3. Key Components of ERM

ERM component	Description
Risk context	An initial component of risk management that describes how an organization frames risk. Establishing the risk context includes defining the organization's risk tolerance and appetite levels.
Risk appetite	The broad-based amount of risk an organization is willing to accept in pursuit of its mission and vision. It is established by the organization's senior-most leadership and serves as the guidepost to set strategy and select objectives.
Risk tolerance	The acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.
Risk management strategy	Outlines how the organization intends to assess, respond to, and monitor risk.
Risk profile	Provides an analysis of the risk that an agency faces toward achieving a strategic objective and identifies appropriate options for addressing significant risks.

Source. NIST SP 800-39; OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

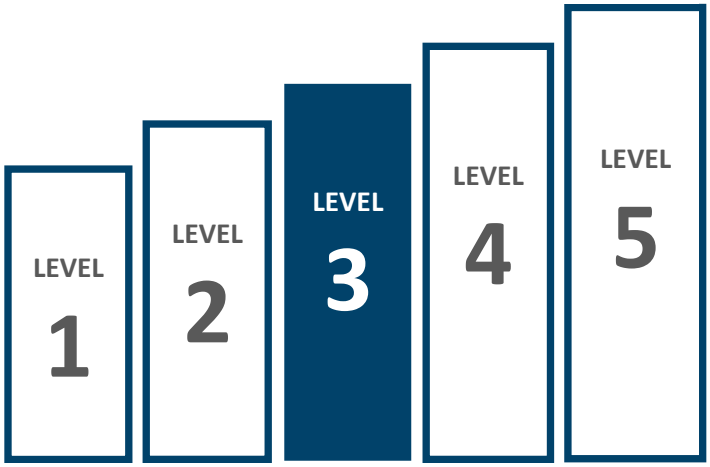
A specific risk that has seen increased focus in the federal government is that from insider threats. Specifically, personnel who are entrusted with sensitive agency data can pose specific types of security risks to organizations, both intentionally and unintentionally. For example, trusted employees 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. The importance of managing risks from insider threats led to the issuance of Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* as well as the *National Insider Threat Policy*.[7] 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.

[7] Exec. Order No. 13,587 (October 7, 2011); Office of the Director of National Intelligence, *National Insider Threat Policy*, November 21, 2012.

Current Security Posture

The Bureau's risk management program is operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level (figure 3). For instance, the Bureau has strengthened its information technology (IT) asset management processes by adopting an IT Asset Management Life Cycle from initial request and acquisition through disposal. Additionally, the Bureau employs automation to track the life cycle of its hardware assets. Further, the Bureau maintains qualitative and quantitative performance measures related to its processes and management of plans of action and milestones, which is also indicative of a higher maturity level.

Figure 3. Risk Management, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

Opportunities for Improvement

Although the Bureau's risk management program is operating at a level-3 (*consistently implemented*) maturity, we identified opportunities to mature the program in the areas of ERM, use of automation to support risk management activities, and insider threat management. We believe that strengthening these areas will allow the Bureau to increase the maturity of its risk management program.

We found that the Bureau has established but not fully implemented its ERM program. In our 2017 FISMA report,[8] we recommended that the Chief Risk Officer continue to work with divisions across the Bureau to ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile. This year, to further comply with OMB Circular A-123, we found that the Bureau has identified enterprisewide risks and developed its risk profile; however, the Bureau is working on determining the impacts and mitigation strategies for the risks. Further, we found that the Bureau has not yet defined key ERM components from OMB Circular A-123, including its risk tolerance levels, or developed its risk appetite statement. Although the Bureau has made progress in establishing its ERM program, we are leaving this recommendation open and will continue to follow up on the Bureau's efforts in this area as part of future FISMA audits.

Additionally, the Bureau has not yet defined how it will use technology, such as a governance, risk management, and compliance tool, at the organizational level to provide a centralized, enterprisewide view of risks. The DHS's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* suggests organizations implement an automated solution across the enterprise that provides a centralized, enterprisewide view of risks, including the integration of all sources of risk information. As mentioned in our 2017 FISMA report, we realize that the implementation

[8] Office of Inspector General, *2017 Audit of the CFPB's Information Security Program*.

of such technologies depends on the Bureau fully implementing its ERM strategy and related components. We believe that the Bureau should begin evaluating technological options that facilitate a consistent and repeatable approach to risk management activities across the organization. As the Bureau is still working on fully implementing its ERM program, we are not making a recommendation in this area at this time. However, we will continue to follow up on the Bureau's efforts as a part of future FISMA audits.

Lastly, our 2016 FISMA report included a recommendation for the CIO to strengthen the agency's risk management processes around insider threats.[9] Specifically, we recommended that the CIO evaluate options and develop an agencywide insider threat program that includes (1) a strategy to raise organizational awareness; (2) an optimal organizational structure; and (3) integration of incident response capabilities, such as ongoing activities around data loss prevention. This year, Bureau officials informed us that the agency has developed a draft Insider Threat Program that they are planning to announce as part of their annual cybersecurity training. Additionally, the Bureau has identified tools that will help support the Insider Threat Program, such as for data loss prevention, which have yet to be implemented. Therefore, we are leaving this recommendation open and will continue to follow up on the Bureau's efforts in this area as a part of future FISMA audits.

Protect

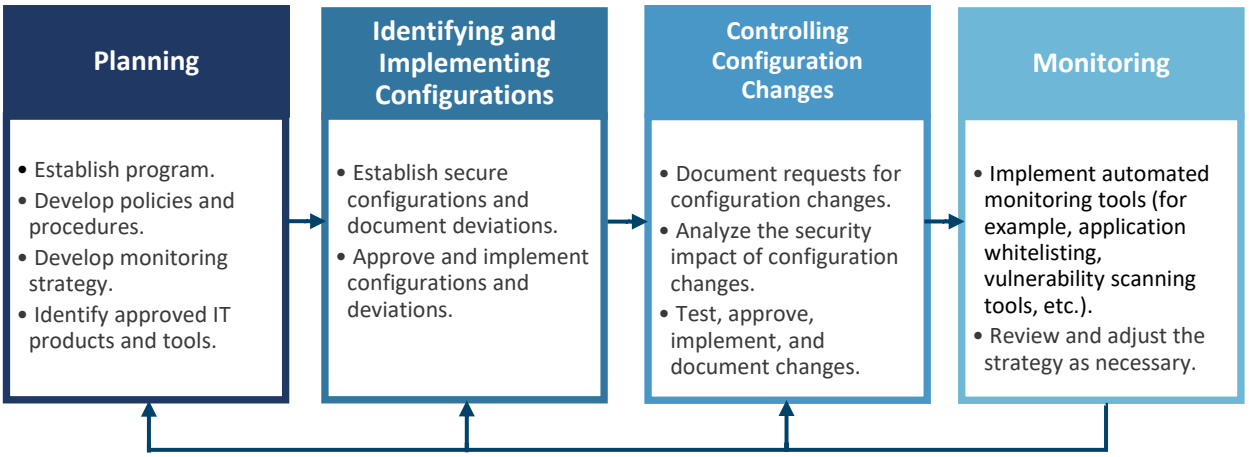
The objective of the *protect* function in the Cybersecurity Framework is to develop and implement safeguards to secure information systems. This function supports the ability to prevent, limit, or contain the impact of a cybersecurity event through applicable configuration management, identity and access management, data protection and privacy, and security training processes.

Configuration Management

FISMA requires agencies to develop an information security program that includes policies and procedures that ensure compliance with minimally acceptable system configuration requirements. Configuration management refers to a collection of activities focused on establishing and maintaining the integrity of products and information systems through the control of processes for initializing, changing, and monitoring their configurations. NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (SP 800-128), recommends integrating information security into configuration management processes. Security-focused configuration management of information systems involves a set of activities that can be organized into four major phases: (1) planning, (2) identifying and implementing configurations, (3) controlling configuration changes, and (4) monitoring (figure 4).

[9] Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*.

Figure 4. Security-Focused Configuration Management Phases



Source. NIST SP 800-128.

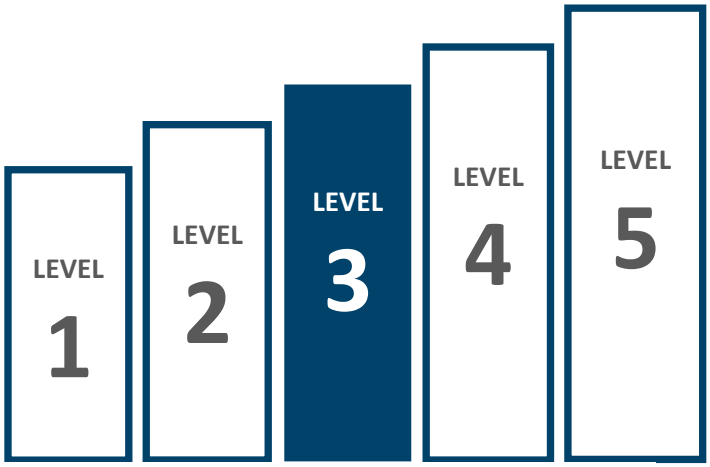
A key component of security-focused configuration management is monitoring, which involves validating that information systems are adhering to organizational policies, procedures, and approved secure configuration baselines. When inconsistencies are identified, the organization should take action to mitigate resulting security risks. Monitoring processes are also needed to identify software security updates and patches that need to be installed for an organization's technology environment. Unpatched or outdated software can expose an organization to increased risk of a cyberattack.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53) states that organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors and that the organization is to establish an organization-defined benchmark for taking corrective actions to remediate flaws identified. In addition, NIST Special Publication 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies*, states that for products and systems, including mobile devices, applying patches corrects security and functionality problems in software and firmware and reduces opportunities for exploitation. It also states that the use of an enterprise mobile device management software is an option to keep mobile device software updated. Further, it states that the software can restrict access if the device's operating system is not up to date.

Current Security Posture

The Bureau's configuration management program is operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level (figure 5). For instance, the Bureau employs network access controls to detect unauthorized hardware. Further, the Bureau tracks and reports on performance measures related to its change control activities.

Figure 5. Configuration Management, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

Opportunities for Improvement

Although the Bureau's configuration management program is operating at a level-3 (*consistently implemented*) maturity, we identified weaknesses in the agency's processes for secure database configurations, vulnerability remediation, and mobile phone patch management. We believe that by strengthening its controls and processes in these areas, the Bureau will be able to increase the maturity of its configuration management program.

Through our vulnerability scanning, we continue to identify weaknesses in the Bureau's database-level security configurations.[10] These weaknesses relate to properly configuring databases to established baselines, audit and accountability, and system and information integrity. Our 2014 FISMA report includes a recommendation for the CIO to strengthen the Bureau's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database- and application-level security configurations.[11] This year, we found that the Bureau has implemented an application-level vulnerability-scanning tool, which the agency is using for its web applications. However, Bureau officials noted that they are in the process of implementing a database-level vulnerability-scanning solution. Although we are not making additional recommendations in this area, we strongly suggest that the Bureau prioritize the implementation of an automated solution and process to periodically assess and manage database-level security configurations. We are leaving this recommendation open and will continue to follow up on the Bureau's efforts in this area as a part of future FISMA reviews.

We also found numerous critical/high-risk vulnerabilities identified in the Bureau's internal vulnerability scans that were not timely remediated. The Bureau's *Information Security Standards* (CS-S-01) requires that critical, high, moderate, and low vulnerabilities be remediated timely, such as less than 30 days for critical vulnerabilities. According to Bureau officials, the key cause for delays is a lack of resources that can be dedicated to remediating identified vulnerabilities. We believe that by ensuring that these

[10] The Bureau provided us with special access and administrative credentials to perform scanning within its internal network.

[11] Office of Inspector General, *2014 Audit of the CFPB's Information Security Program*.

vulnerabilities are remediated timely, the Bureau will be able to better protect its information systems from internal and external threats.

Further, we found that the Bureau is not enforcing the application of current patch levels for the operating system of its mobile phones. Specifically, we identified mobile devices that do not have current operating system patches applied. The Bureau's *Technology & Innovation Patch Management Process* requires that patches and updates that are critical to the functionality and security of the Bureau's software be installed safely and timely. The process requires that patches are identified, assessed, tested, deployed, and monitored. The key contributing factor for the outdated operating system patches is that the Bureau has not enabled the capability to enforce this level of patching/updating within its mobile device monitoring tool. We believe that by ensuring the timely application of patches and security updates for its mobile phones, the Bureau will decrease the risk of exploitation on its mobile devices.

Recommendations

We recommend that the CIO

1. Strengthen configuration management processes by
    a. Remediating configuration-related vulnerabilities in a timely manner.
    b. Ensuring that optimal resources are allocated to perform vulnerability remediation activities.
2. Develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.

Management's Response

In response to our draft report, the CIO concurs with our recommendations. The CIO notes that in 2019, the agency will ensure that configuration-related vulnerabilities are efficiently tracked and mitigated and that adequate resources are prioritized to support configuration-related vulnerability remediation efforts. Further, the CIO notes that the Bureau will deploy a unified endpoint management solution, which will enable system administrators to centrally manage updates and patches for mobile devices.

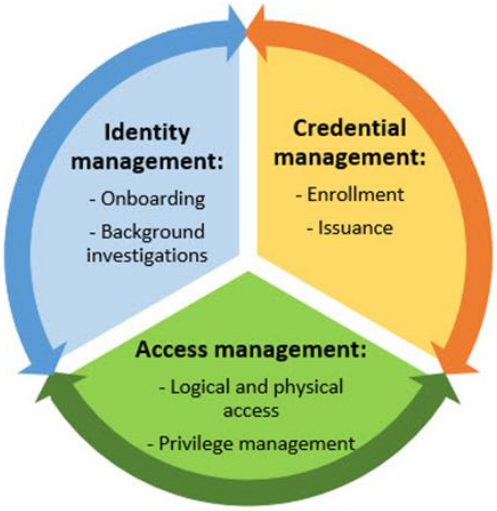
OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendations. We plan to follow up on the Bureau's actions to ensure that the recommendations are fully addressed.

Identity and Access Management

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*. Supporting activities include onboarding and personnel screening, issuing and maintaining user credentials, and managing logical and physical access privileges, which are collectively referred to as identity, credential, and access management (ICAM) (figure 6).

Figure 6. ICAM Conceptual Design



Source. CIO Council, *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance.*

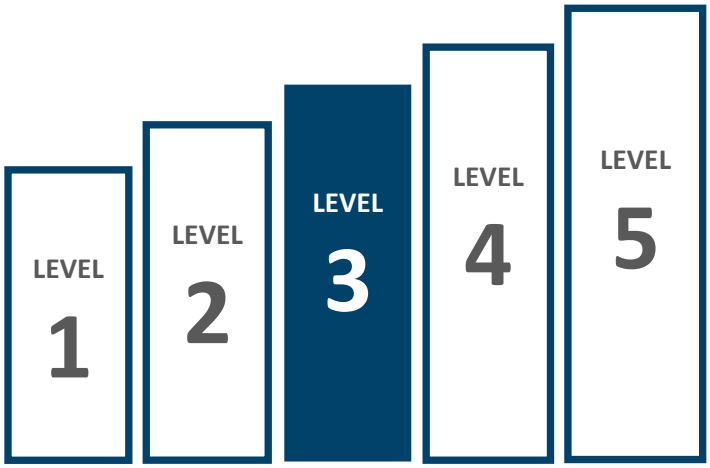
A key component of effective identity and access management is developing a comprehensive strategy that outlines the components of the agency's ICAM program within the business functions that they support. The *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance* provides the government with a common framework and implementation guidance to plan and execute ICAM programs. Another 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 SP 800-53 emphasizes the importance of tracking and controlling access privileges and ensuring that these privileges are periodically reviewed and adjusted.

In support of federal ICAM requirements, the Bureau has developed and implemented policies and procedures that cover multiple functions throughout the life cycle of a user's digital identity. For example, the Bureau's policies and procedures cover requirements for account management, multifactor authentication, audit logging, background investigations, and onboarding. With respect to the control of privileged accounts, the Bureau's policies and procedures require privileged users to annually resubmit their signed and approved user-access forms and rules of behavior or their privileged access will be revoked.

Current Security Posture

The Bureau's identity and access management program is operating at level 3 (*consistently implemented*), with the agency effectively implementing configuration/connection requirements for remote access management (figure 7). Specifically, the Bureau has effectively implemented controls to ensure that end-user devices are appropriately configured before allowing remote access. Further, the Bureau ensures that individuals are restricted in their ability to transfer data accessed remotely to unauthorized devices.

Figure 7. Identity and Access Management, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

We also found that as part of its ICAM program, the Bureau has defined roles and responsibilities at the organizational and system levels for stakeholders, is working to consolidate ICAM investments across the agency, and has defined an implementation strategy. The Bureau continues to meet milestones to implement automated tools used to help monitor ICAM activities.

Opportunities for Improvement

Although the Bureau's identity and access management program is operating at a level-3 (*consistently implemented*) maturity, we identified opportunities for improvement in the areas of maintaining annual privileged access agreement certification forms and requiring the use of multifactor authentication sign-on for Bureau users. We believe that by strengthening its controls and processes in these areas, the Bureau will be able to increase the maturity of its identity and access management program.

Although the Bureau is ensuring that user-access agreements and rules of behavior for individuals with privileged access are completed before access is granted to Bureau systems and applications, the Bureau is not consistently managing and updating this documentation in accordance with Bureau and NIST 800-53 requirements. Specifically, we found that for a sample of 15 privileged/administrative users, 7 had not annually recertified their user-access agreements and rules-of-behavior forms. The Bureau's *Elevated/Privileged User Standard Operating Procedure* states that privileged users are required to submit a new user-access form annually. Additionally, the *Rules of Behavior for Privileged User Policy* (CS-S-03) requires that Bureau-authorized privileged users recognize, acknowledge, and adhere to the additional responsibilities associated with their elevated access to Bureau information systems by signing a statement of acceptance before being issued a privileged account. We identified similar issues in this area and issued recommendations in the 2016 FISMA audit report and in a 2018 security control review.[12]

[12] The recommendation issued during the 2016 FISMA review was closed during our 2017 FISMA review. The recommendation issued during the 2018 security control review remains open.

Privileged accounts have elevated permissions that allow users to access or alter system functions, configurations, and data; therefore, these accounts could pose significant risk to Bureau IT systems and sensitive information if mismanaged or compromised. The Bureau has cited a lack of resources as a contributing factor for this continuing to be an issue. We believe that by enforcing its access control process, the Bureau can achieve greater assurance that personnel are maintaining their privileged access on a need-to-know basis and 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.

In our 2017 FISMA audit report, we found that the Bureau enabled the option for both privileged and nonprivileged users to use their personal identity verification (PIV) cards to access their computers when at the Bureau; however, it was not a requirement.[13] We recommended that the CIO develop and implement a tiered approach for implementing multifactor authentication that considers system risk levels and user roles and uses lessons learned to inform broader adoption. This year, we found that the use of PIV to sign on to Bureau systems still remains an option for users but is not required. The Bureau continues to implement its ICAM Roadmap initiatives, which includes using PIV cards for privileged and nonprivileged users. Further, Bureau officials stated that the key cause for not requiring the use of PIV to sign on to Bureau systems is that the agency has made a strategic decision to go from a network-based to a cloud-based infrastructure and plans to evaluate ICAM initiatives accordingly. As such, we are leaving this recommendation open and will continue to follow up on the Bureau's efforts as a part of future FISMA audits.

Recommendation

We recommend that the CIO

3. Determine whether established processes and procedures for management of user-access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.

Management's Response

In response to our draft report, the CIO concurs with our recommendation and notes that the Bureau will implement an IT service management tool that will integrate with user account provisioning functions to ensure consistent procedural and technical access controls. Until the tool is implemented, the Bureau will incorporate additional workflow controls to further mature this process and ensure that adequate resources are assigned to make changes as needed.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendation. We plan to follow up on the steps outlined in the Bureau's response to ensure that the recommendation is fully addressed.

[13] Office of Inspector General, *2017 Audit of the CFPB's Information Security Program.*

Data Protection and Privacy

Data protection and privacy refers to a collection of activities focused on the security objective of confidentiality, preserving authorized restrictions on information access, and disclosure to protect personal privacy and proprietary information. In today's digital world, effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their personally identifiable information (PII) increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, OMB Circular A-130, *Managing Information as a Strategic Resource*, requires federal agencies to develop, implement, and maintain agencywide privacy programs that, where PII is involved, play a key role in information security and implementing the NIST Risk Management Framework. Although the head of each federal agency remains ultimately responsible for ensuring that privacy interests are protected and for managing PII responsibly within their respective agency, Executive Order 13719, *Establishment of the Federal Privacy Council*, requires agency heads to designate a senior agency official for privacy who has agencywide responsibility and accountability for the agency's privacy program.

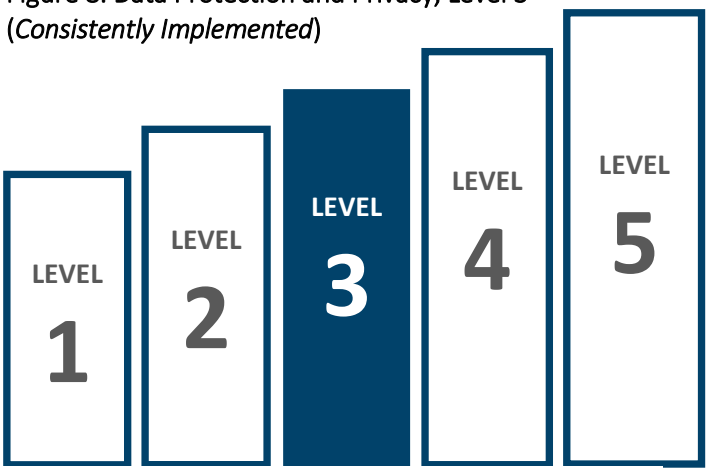
NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (SP 800-122), notes the importance of the identification of all PII residing in the organization or under the control of a third party on behalf of the organization. Further, SP 800-122 recommends measures to protect PII and other sensitive information, including operational safeguards (for example, policies, procedures, and awareness training), privacy-specific safeguards (for example, minimizing the use, collection, and retention of PII), and security controls (for example, access control to PII, media sanitization, and the protection of data at rest or in transit).

To meet its mission of regulating the offerings and provisions of consumer financial products and services under federal consumer financial laws and to educate and empower consumers to make better-informed financial decisions,[14] the Bureau collects a significant amount of sensitive PII. This information includes consumer financial data on credit card accounts, mortgage loans, arbitration case records, automotive sales, credit scores, private student loans, and storefront payday loans.

Current Security Posture

The Bureau's data protection and privacy program is operating at level 3 (*consistently implemented*), though the agency is also performing remote wiping of mobile devices, which is associated with a higher maturity level (figure 8). We found that privacy policies and procedures have been defined and communicated. The Bureau has also implemented Federal Information Processing Standard–validated encryption for sensitive data and restricts use of removable devices.

Figure 8. Data Protection and Privacy, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

[14] 12 U.S.C. §§ 5491(a), 5493(d).

In addition, the Bureau has established and maintains a privacy program to provide for the development and maintenance of privacy controls. The program includes a dedicated staff headed by a senior agency official for privacy. Further, the privacy team works closely with IT staff and other stakeholders as needed for security of sensitive data. The Bureau has implemented annual privacy training and has a privacy breach response plan in place.

Opportunities for Improvement

Although we found that the Bureau's privacy program was operating at a level-3 (*consistently implemented*) maturity, we identified opportunities to mature the program to ensure that it is effective. Specifically, we found that the Bureau had not appropriately restricted sensitive consumer and employee information contained in an internal collaboration tool, and the agency had not ensured that all appropriate datasets are included in its inventory of PII. We believe that by strengthening its controls and processes in these areas, the Bureau will be able to increase the maturity of its data protection and privacy program.

We found that access controls were not appropriately set for an internal collaboration tool, resulting in sensitive consumer and employee information (including PII) available to internal users who did not have a valid need to know. The Bureau's *Handbook for Sensitive Information* states that sensitive information should not be disclosed to any Bureau employee or contractor unless that person has a need to know and authority to access the information. In addition, NIST SP 800-122 notes that organizations can enforce the most restrictive set of rights and privileges or accesses needed by users for the performance of specified tasks. Concerning PII, the organization can ensure that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges.

A key cause for this issue is that the Bureau's administration of the internal collaboration tool is decentralized; however, administrators in Bureau divisions do not have specialized skills or receive training on the collaboration tool's available access restriction capabilities. Another cause is that the logs are retained for the collaboration tool but are not reviewed. By appropriately restricting information to internal users, the Bureau may reduce the insider threat risk of exposing sensitive consumer and employee information to those without a valid need to know. After we notified the Bureau of these issues, the agency took immediate actions to restrict access and developed a plan of action and milestones to further strengthen controls.[15]

In February 2018, we issued a report on the Bureau's privacy program that included two recommendations.[16] One recommendation related to the physical security of equipment and documents, and the other recommendation referred to an incomplete inventory of PII that the Bureau is collecting or handling, who within the Bureau is responsible for the security of the data, where the information is stored, and whether a privacy impact assessment or System of Record Notice is required. During our 2018 FISMA fieldwork, we found that the Bureau had taken steps to address both these recommendations. For the recommendation related to the physical security of devices, we found that the Bureau had made some progress on the issue, including providing new cable locks for equipment. Related

[15] The detailed results of our follow-up work in this area will be transmitted to the Bureau under a separate, restricted cover because of the sensitive nature of the information.

[16] Office of Inspector General, *Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program*, OIG Report 2018-IT-C-003, February 14, 2018.

to the PII inventory recommendation, we found that the Bureau was working to incorporate human resources datasets into the PII inventory. Both issues remain open at this time. As such, we are leaving these two recommendations open and will continue to follow up on the Bureau's efforts as a part of future audits.

Recommendation

We recommend that the CIO

4. Ensure that the Bureau's existing information security continuous monitoring approach is implemented for an internal collaboration tool to appropriately restrict and monitor access.

Management's Response

In response to our draft report, the CIO concurs with our recommendation. The CIO notes that the Bureau will continue to prioritize a project to protect unstructured data within the internal collaboration environment and that the technology will provide visibility into end-user access to sensitive data and prompt any remedial action.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendation. We plan to follow up on the Bureau's actions to ensure that the recommendation is fully addressed.

Security Training

FISMA requires agencies to develop an information security program that provides security awareness training to personnel, including contractors, who support the operations and assets of the organization, as well as role-based training for individuals with significant information security responsibilities. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, notes that, in general, people are one of the weakest links in attempting to secure agency systems and networks. As such, a robust, enterprisewide security awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

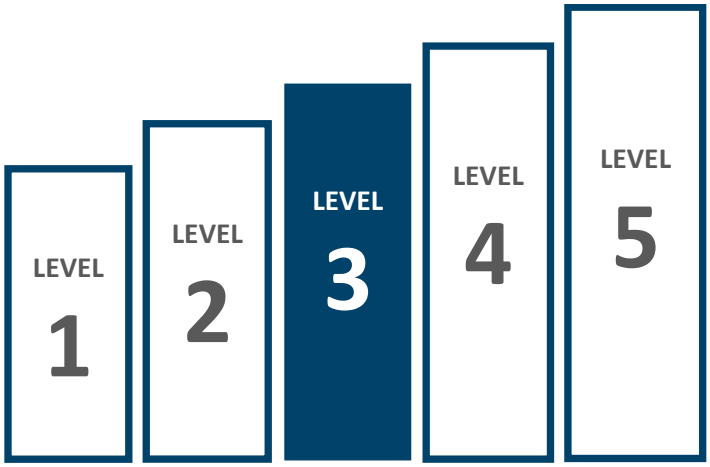
In accordance with FISMA requirements, the Bureau's information security policy states that all employees and contractors with access to agency information systems must receive security awareness training before being permitted access to the Bureau network and each year thereafter. The policy also requires that role-based training be provided for individuals with significant security responsibilities and that records of awareness and role-based training be maintained.

NIST has issued the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, which is a coordinated national effort focused on cybersecurity awareness, education, training, and professional development. The NICE framework allows organizations to map their cybersecurity workforce into seven categories based on specialty areas and roles. These general roles are then used to tailor training needs for staff, depending on what functions they perform. The Bureau is using the NICE framework for its role-based training and has completed mapping its IT staff to specific categories and deployed role-based training aligned to the NICE framework.

Current Security Posture

The Bureau's security awareness and training program is operating at level 3 (*consistently implemented*) (figure 9). For example, the Bureau leverages an automated security awareness training solution for employees and contractors, posts cybersecurity tips of the week on its intranet, and participates in other cybersecurity awareness activities throughout the year. In addition, the Bureau ensures that individuals with significant security responsibilities are provided with specialized security training before they access information systems or perform assigned duties and periodically thereafter. Moreover, in 2018 the Bureau completed a mapping of its IT employee types to respective NIST NICE training categories.

Figure 9. Security Training, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

Opportunities for Improvement

Although we found that the Bureau's security training program is operating at a level-3 (*consistently implemented*) maturity, we identified opportunities to mature the program to ensure that it is effective. Specifically, we found that the Bureau has not completed deployment of its phishing program across the agency or conducted a skills gap analysis for employees with cybersecurity responsibilities. We believe that by strengthening its controls and processes in these areas, the Bureau will be able to increase the maturity of its security training program.

In our 2017 FISMA audit, we recommended that that the Bureau conduct periodic phishing exercises to measure the effectiveness of its information security awareness and training activities.[17] This year, we found that although the Bureau has begun deploying a phishing program and evaluated results of the limited exercises, the phishing program has not been deployed Bureauwide. Therefore, we are leaving this recommendation open and will continue to monitor the Bureau's progress in this area as part of our future FISMA audit activities.

In addition, we believe that the Bureau should continue to refine its role-based training by conducting a skills gap analysis for its IT employees and incorporating the results into its training strategy. The NICE framework states that conducting such an assessment allows an agency to identify training that will allow existing staff members to address identified gaps. Bureau officials stated that they plan to conduct such an analysis in 2019. As such, we are not making a recommendation in this area and will continue to monitor the Bureau's progress as part of our future FISMA audit activities.

[17] Office of Inspector General, *2017 Audit of the CFPB's Information Security Program.*

Detect

The objective of the *detect* function in the Cybersecurity Framework is to implement activities to discover and identify the occurrence of cybersecurity events in a timely manner. The Cybersecurity Framework notes that continuous monitoring processes are used to detect anomalies and changes in the organization's environment of operation and maintain knowledge of threats and security control effectiveness.

Information Security Continuous Monitoring

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. 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 notes that a key component of an effective ISCM program is a comprehensive ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission and business impacts.

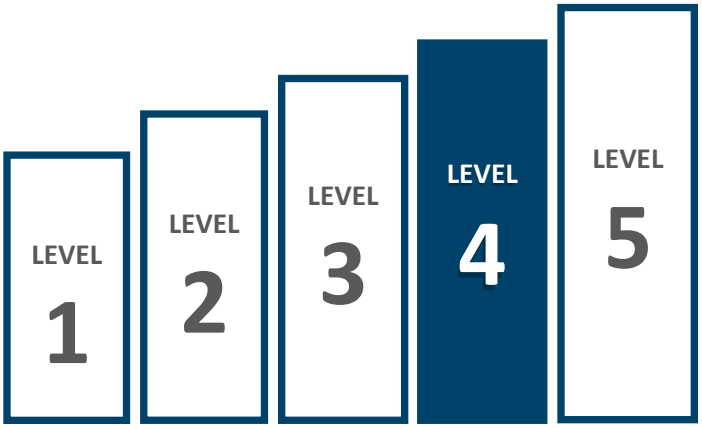
SP 800-137 emphasizes that an ISCM strategy is meaningful only within the context of broader organizational needs, objectives, or strategies, and as part of a broader risk management strategy. Once a strategy is defined, SP 800-137 notes that the next step in establishing an effective ISCM program is to establish and collect security-related metrics to support risk-based decisionmaking throughout the organization. An ISCM strategy is periodically reviewed to ensure that it sufficiently supports the organization in operating within acceptable risk tolerance levels, that metrics remain relevant, and that data are current and complete.

To further enhance the government's ISCM capabilities, Congress established the Continuous Diagnostics and Mitigation (CDM) program. The CDM program provides agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Current Security Posture

We found that the Bureau's ISCM program continues to operate at level 4 (*managed and measurable*), which represents an effective level of maturity (figure 10). This year, we found that the Bureau has made several improvements to its ISCM program. For instance, we found that the Bureau has enhanced the functionality of its information security information and event-monitoring tool by tracking emails being sent to external sources and identifying web traffic anomalies. Additionally, the Bureau has implemented continuous monitoring

Figure 10. ISCM, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

tools that perform malware detection and web application scanning.

Opportunities for Improvement

Although the Bureau's ISCM program is operating at a level-4 (*managed and measurable*) maturity, we identified opportunities to improve the program to ensure that it remains effective. Specifically, we note that the agency's ISCM strategy and supporting processes will need to be updated as the agency's ERM program is formalized and implemented and as the CDM program becomes available.

In our 2017 FISMA audit and again this year, we found that the Bureau had not developed an agencywide risk management strategy to help ensure that risks across the organization are consistently assessed, prioritized, and monitored over time.[18] Once the risk management strategy has been updated, the agency will need to update its ISCM program and supporting processes accordingly. In addition, as detailed in the Configuration Management section above, we continue to find opportunities to strengthen the Bureau's vulnerability management practices for its databases. Addressing these areas will help the Bureau maintain and improve the maturity of its ISCM program and provide it with greater visibility into the effectiveness of supporting processes. We will continue to monitor the Bureau's progress in developing and implementing a risk management strategy and maturing its ISCM program as part of our future FISMA audits.

Further, we found that the Bureau can mature its ISCM program and capabilities by using the CDM program where appropriate. Through the CDM program, DHS provides federal agencies with capabilities and tools that help identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. In 2018, Bureau officials stated that they are still working with DHS to obtain ISCM tools and have received waivers to use some of the Bureau's existing tools. Additionally, Bureau officials are evaluating whether the CDM program will support their target architecture. The Bureau's 2022 target architecture is migrating to a cloud-only infrastructure, accelerating adoption of cloud email and collaboration tools, and improving security shared services. We will continue to monitor the Bureau's progress in implementing the capabilities of the CDM program as part of our future FISMA audits.

Respond

The objective of the *respond* function in the Cybersecurity Framework is to implement processes to contain the impact of detected cybersecurity events. Activities include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities.

Incident Response

FISMA requires each agency to develop, document, and implement an agencywide information security program that includes policies and procedures for incident response. Best practices for incident response are detailed in NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*, which notes that an incident response process consists of four main phases: preparation; detection and

[18] Office of Inspector General, *2017 Audit of the CFPB's Information Security Program.*

analysis; containment, eradication, and recovery; and postincident activity (table 4). It further notes that establishing an incident response capability should include creating an incident response policy and plan; developing procedures for performing incident handling and reporting; and establishing relationships and lines of communications between the incident response team and other groups, both internal and external to the agency.

Table 4. Key Incident Response Phases

Incident response phase	Description
Preparation	Establish and train the incident response team and acquire the necessary tools and resources.
Detection and analysis	Detect and analyze precursors and indicators. A precursor is a sign that an incident may occur in the future, and an indicator is a sign that an incident may have occurred or is occurring currently.
Containment, eradication, and recovery	Contain an incident to limit its impact, gather and handle evidence, eliminate components of the incident, and restore affected systems to normal operations.
Postincident activity	Capture lessons learned to improve security measures and the incident response process.

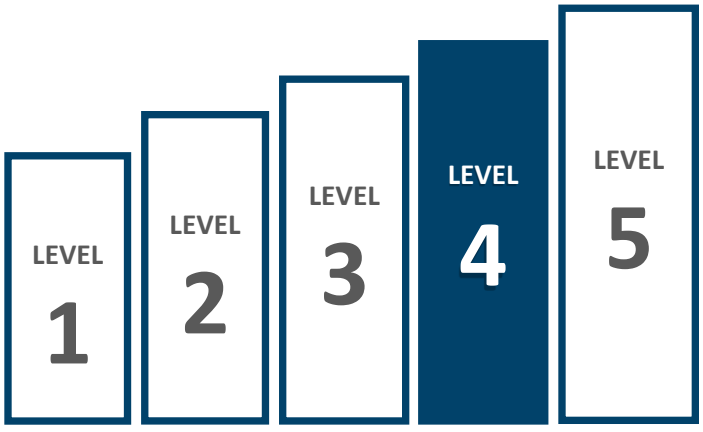
Source. NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide.*

The Bureau's Incident Response Program documents the procedures for addressing the detection, response, and reporting of information security incidents related to Bureau data and resources. The procedures include scope, roles and responsibilities, incident notification and escalation tasks, external reporting requirements, and a threat vector taxonomy. The Bureau also coordinates with DHS for incident response capabilities.

Current Security Posture

We found that the Bureau has matured its incident response program from level 3 in 2017 to level 4 (*managed and measurable*), which represents an effective level of maturity (figure 11). The Bureau has matured several incident response capabilities; for instance, it is using multiple incident response tools, such as a profiling tool that establishes a baseline of network activity and identifies anomalies, and a central automated solution, which is used to detect and analyze incidents. Additionally, this year the Bureau implemented several incident response metrics.

Figure 11. Incident Response, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

Opportunities for Improvement

Although the Bureau has implemented an effective incident response program, we identified opportunities to improve the program to ensure that it remains effective. Specifically, we found that the Bureau's technical points of contact for formally declaring a cybersecurity incident to DHS are not up to

date. In addition, our previous work has identified improvements needed to ensure that alerts and logs from applications residing in the Bureau's new cloud computing environment are uploaded to the agency's central automated solution. We believe that by strengthening its controls and processes in these areas, the Bureau will be able to maintain an effective incident response program.

We found that the Bureau's technical points of contact are not up to date for the Standing Federal Network Authorization, which authorizes specific individuals to formally declare a cybersecurity incident to DHS on behalf of the Bureau. OMB Memorandum M-16-03 requires that the technical points of contact related to the Standing Federal Network Authorization be updated as necessary.[19] We believe that a key contributing factor for this issue was that there is no process to update the Standing Federal Network Authorization. By keeping the points of contact up to date, the Bureau will not be limiting the individuals who are allowed to formally declare a cybersecurity incident to DHS on behalf of the Bureau. Not doing so could also hamper the agency's ability to receive timely support from DHS. After the conclusion of our fieldwork, the Bureau took steps to update the points of contact for the Standing Federal Network Authorization. As such, we are not making a recommendation in this area.

In our 2017 FISMA audit report, we recommended that the CIO ensure applicable alerts and logs from applications residing in the Bureau's new cloud computing environment are uploaded to the agency's central automated solution, which is used to detect and analyze incidents.[20] In conducting follow-up work, we found that the Bureau is still working on an automated solution to this issue. Therefore, we are leaving this recommendation open and will continue to monitor the Bureau's progress in this area as part of our future FISMA audit activities.

Recover

The objective of the *recover* function in the Cybersecurity Framework is to ensure that organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The Cybersecurity Framework outlines contingency planning processes that support timely recovery to normal operations and reduce the impact of a cybersecurity event.

Contingency Planning

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 organization. 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. NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, provides best practices for information system contingency planning. It highlights the importance of conducting a business impact analysis, which helps identify and prioritize information systems and components critical to supporting the organization's mission and business processes, as a foundational step to effective contingency planning. A business impact analysis allows an

[19] OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements,* October 30, 2015.

[20] Office of Inspector General, *2017 Audit of the CFPB's Information Security Program*.

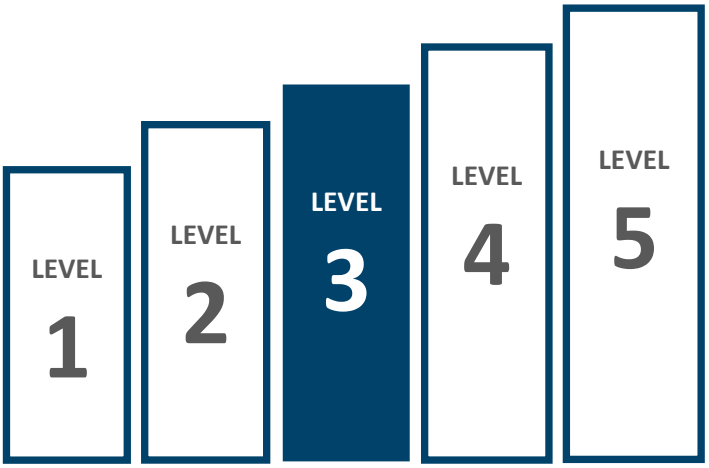
organization to measure priorities and interdependencies (internal or external to the entity) by risk factors that could affect mission-essential functions.

An additional important factor for information system contingency planning, noted in NIST SP 800-53, is its integration with other function areas. NIST SP 800-53 highlights the importance of closely coordinating contingency planning with incident handling activities so that organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. For information system contingency planning, it is important to put in place procedures to use the results of contingency testing as part of an ERM program to make risk-based decisions at an enterprise level.

Current Security Posture

The Bureau's contingency planning program is operating at level 3 (*consistently implemented*) (figure 12). For instance, the Bureau has defined and communicated roles and responsibilities for contingency planning and reinforces these during individual system contingency testing. Additionally, the Bureau has established teams to implement contingency planning strategies and has implemented its processes for system backup and storage.

Figure 12. Contingency Planning, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

Opportunities for Improvement

Although the Bureau's contingency planning program is operating at a level-3 (*consistently implemented*) maturity, we identified opportunities to mature the program to ensure that it is effective through the completion of a business impact analysis, use of contingency testing results to better inform risk-based decisions, and integration of contingency planning development and maintenance activities with other stakeholders. We believe that by strengthening its controls and processes in these areas, the Bureau will be able to maintain an effective contingency planning program.

In our 2016 FISMA audit report, we recommended that the CIO strengthen the Bureau's contingency program by performing an agencywide business impact analysis and updating the agency's continuity of operations plan and IT contingency plan accordingly.[21] This year, similar to 2017, Bureau officials informed us that work is underway toward completing a business impact analysis; however, there is no timeline for completion. Therefore, we are leaving this recommendation open and will continue to monitor the Bureau's progress in this area as part of our future FISMA audit activities.

Further, we found that although the Bureau is using system contingency plan testing results to improve future testing activities, the agency does not have processes in place to use the results of contingency testing to make risk-based decisions at an enterprise level. Bureau officials informed us that once the

[21] Office of Inspector General, *2016 Audit of the CFPB's Information Security Program.*

agency's ERM program has been fully implemented, contingency planning documentation and processes will be updated accordingly. Additionally, although the Bureau has coordinated contingency testing with its incident response team, we found that the agency does not integrate plan development or maintenance activities with other continuity areas, such as occupant emergency. We are not making additional recommendations in this report related to contingency planning because of the Bureau's continuing efforts to establish an ERM program. We will continue to monitor the Bureau's progress in maturing its contingency planning program as part of future FISMA audits.

Status of Prior Years' Recommendations

As part of our annual FISMA audit, we reviewed the actions taken by the Bureau to address the outstanding recommendations from our prior years' FISMA reviews. Below is a summary of the status of the 10 recommendations that were open at the start of our 2018 FISMA audit (table 5). Based on corrective actions taken by the Bureau, we are closing 3 prior recommendations related to identity and access management, incident response, and contingency planning. The remaining 7 recommendations related to risk management, configuration management, identity and access management, incident response, and contingency planning will remain open. We will continue to monitor the Bureau's progress in addressing the 7 open recommendations as a part of future FISMA reviews.

Table 5. Status of Prior Years' Recommendations

Recommendation	Status	Disposition
Risk management		
In our 2016 FISMA audit report, we recommended that the CIO evaluate options and develop an agencywide insider threat program to include (1) a strategy to raise organizational awareness; (2) an optimal organizational structure; and (3) integration of incident response capabilities, such as ongoing activities around data loss prevention.	Open	The Bureau has developed an insider threat policy; however, planned automated tools have yet to be deployed and the policy has not been implemented.
In our 2017 FISMA audit report, we recommended that the Chief Risk Officer continue to work with divisions across the Bureau to ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.	Open	Although the Bureau has made progress in establishing its ERM program, it has not developed its risk appetite statement or risk tolerance levels.
Configuration management		
In our 2014 FISMA audit report, we recommended that the CIO strengthen the Bureau's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.	Open	The Bureau has implemented an automated solution for assessing application-level security configurations for web applications, but has not done so for assessing and managing database security configurations.

Recommendation	Status	Disposition
Identity and access management		
In our 2017 FISMA audit report, we recommended that the Chief Operating Officer ensure that all contractors performing IT functions have background investigations initiated before onboarding.	Closed	This year we found that the Bureau is ensuring that contractors receive background investigations before onboarding. Further, once hired, the Bureau is ensuring that contractors' full background investigations are started with the Office of Personnel Management.
In our 2017 FISMA audit report, we recommended that the CIO develop and implement a tiered approach for implementing multifactor authentication that considers system risk levels and user roles and uses lessons learned to inform broader adoption.	Open	The Bureau does not require privileged and nonprivileged users to authenticate to its internal network using multifactor authentication.
Security training		
In our 2017 FISMA audit report, we found that the Bureau did not conduct periodic phishing exercises to measure the effectiveness of its information security awareness and training activities.	Open	Although the Bureau has implemented a phishing program, it has not rolled the program out agencywide and incorporated analysis of prior phishing exercises into new exercises.
Incident response		
In our 2017 FISMA audit report, we recommended that the CIO ensure applicable alerts and logs from applications residing in the Bureau's new cloud computing environment are uploaded to the agency's central automated solution, which is used to detect and analyze incidents.	Open	The Bureau is in the process of developing a solution to address this recommendation.
In our 2017 FISMA audit report, we recommended that the CIO ensure that containment strategies are developed and implemented for the key types of incidents applicable to the Bureau's environment.	Closed	The Bureau has developed and implemented containment strategies for the key types of incidents applicable to the agency.

Recommendation	Status	Disposition
Contingency planning		
In our 2016 FISMA audit report, we recommended that the CIO strengthen the Bureau's contingency program by performing an agencywide business impact analysis and updating the agency's continuity of operations plan and IT contingency plan to reflect the results of the business impact analysis and the current operating environment of the Bureau.	Open	The Bureau is in the process of completing a business impact analysis.
In our 2017 FISMA audit report, we recommended that the CIO ensure that contingency plans for all Bureau systems are tested, as appropriate; contingency testing is integrated with the testing of related plans, such as those for incident response and continuity of operations, to the extent practicable; and testing results are used to improve related processes, as needed.	Closed	Contingency plans for all the Bureau's systems are tested or scheduled, as appropriate. Additionally, contingency testing is integrated with incident response activities. Further, testing results are used to improve future exercises.

Source. OIG analysis.

Appendix A: Scope and Methodology

Our specific audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. To accomplish our objectives, we reviewed the effectiveness of the Bureau's information security program across the five function areas outlined in DHS's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*: *identify*, *protect*, *detect*, *respond*, and *recover*. These five function areas consist of eight security domains: risk management, configuration management, identity and access management, data protection and privacy, security training, ISCM, incident response, and contingency planning. To assess the Bureau's information security program, we interviewed Bureau management and staff; analyzed security policies, procedures, and documentation; performed vulnerability scanning; and observed and tested specific security processes and controls. We also assessed the implementation of select security controls for cloud-based systems.

To rate the maturity of the Bureau's information security program and functional areas, we used the scoring methodology defined in DHS's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. The maturity ratings are determined by a simple majority, where the most frequent level (that is, the mode) across the metrics serves as the overall rating.

We performed our fieldwork from May 2018 to September 2018. 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

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

October 25, 2018

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

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the *2018 Audit of the BCFP's Information Security Program*. We are pleased that you found that the Bureau's information security program is operating at an overall level 3 (consistently implemented) maturity and certain components of the program operating at a level 4 (managed and measurable) maturity based on the OIG Federal Information Security Modernization Act of 2014 (FISMA) maturity model. In fiscal year (FY) 2019, the Bureau will continue to enhance its processes and technologies in an effort to continue to raise our overall maturity level and address each recommendation cited in the draft report.

Furthermore, we recognize that the draft report states the following and the Bureau offers responses to these statements:

- The BCFP is operating at a level 3 maturity for the **Identify** function. The Bureau's risk management program is operating at level 3 (*consistently implemented*). In FY 2018, the Bureau has strengthened its information technology (IT) asset management processes by adopting an IT Asset Management Life Cycle from initial request and acquisition through disposal. Additionally, the Bureau employs automation to track the life cycle of its hardware assets. The Bureau maintains qualitative and quantitative performance measures related to its processes and management of plans of action and milestones (POA&M), which is also suggestive of a higher maturity level. In FY 2019, the Bureau will continue to mature its risk management program to fully implement agency-wide its Enterprise Risk Management (ERM) program and Insider Threat Program.

consumerfinance.gov

- The BCFP operates at a level three maturity for the **Protect** function. The Bureau's configuration management program is operating at level 3 (*consistently implemented*). The Bureau employs network access controls to detect unauthorized hardware. Additionally, the Bureau tracks and reports on performance measures related to its change control activities. We acknowledge the need to mature/strengthen the Bureau's vulnerability management program. In FY 2019, the Bureau will continue to prioritize the implementation of an automated solution and process to periodically assess and manage database-level security configurations.

- The BCFP **Identity and Access Management (ICAM)** program is operating at level 3 (*consistently implemented*). The Bureau has effectively implemented configuration/connection requirements for remote access management including specific controls that ensure end-user devices are appropriately configured prior to allowing remote access. The Bureau continues to meet milestones to implement automated tools used to help monitor ICAM activities. In FY 2019, the Bureau will continue to focus on applying a tiered approach for implementing multifactor authentication.

- The BCFP **Bureau's Data Protection and Privacy** program is operating at level 3 (*consistently implemented*), with the agency performing remote wiping of mobile devices, which is associated with a higher maturity level. Privacy policies and procedures have been defined and communicated. The Bureau has also implemented Federal Information Processing Standard–validated encryption for sensitive data and restricts use of removable devices. In addition, the Bureau has established and maintains a privacy program to provide for the development and maintenance of privacy controls. The program includes a dedicated staff headed by a senior agency official for privacy. In FY 2019, the BCFP Privacy team will continue to work closely with information technology staff and other stakeholders as needed regarding the privacy and protection of the Bureau's data.

- The BCFP **Security Training** program is operating at level 3 (*consistently implemented*). The Bureau leverages an automated security awareness training platform for employees and contractors, posts cybersecurity tips of the week on its intranet, and participates in other cybersecurity awareness activities throughout the year. In addition, the Bureau ensures that individuals with significant IT security responsibilities are provided with role-based security training before provisioning of information system access or performance of assigned duties and periodically thereafter. In FY 2019, the Bureau will complete the deployment of the phishing protection program across the agency and an analysis of skill gaps for prioritized cybersecurity personnel.

- The BCFP's **Detect** function and our information security continuous monitoring (ISCM) program continues to operate at level 4 (managed and measurable). The Bureau has made several improvements to its ISCM program since FY 2017. For instance, the Bureau has enhanced the functionality of its security information and event-monitoring tool by tracking emails being sent to external sources and identifying web traffic anomalies in addition to implementing continuous monitoring tools that perform malware detection and web application scanning.

- The BCFP's **Respond** function has matured its incident response program from level 3 (in 2017) to level 4 (*managed and measurable*) in FY 2018. The Bureau has matured several incident response capabilities. For instance, the agency is using multiple incident response tools including a profiling tool that establishes a baseline of network activity and identifies anomalies, and a central automated solution which is used to detect and analyze incidents. Additionally, the Bureau began tracking several incident response metrics in FY 2018.

- The BCFP's **Recover** function is operating at a level 3 maturity. The Bureau has defined and communicated roles and responsibilities for contingency planning and reinforces these during individual system contingency testing. Additionally, the Bureau has established teams to implement contingency planning strategies and has fully implemented its processes for system backup and storage. We have shared with you the Bureau's efforts toward completing an agency wide Business Impact Analysis (BIA). In FY 2019, the Bureau will continue to prioritize these efforts.

We appreciate the OIG noting our progress on remediating recommendations from previous OIG reviews. We value your objective, independent viewpoints and consider you to be a trusted source of informed, accurate, and insightful information.

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,

KATHERINE SICKBERT Digitally signed by KATHERINE SICKBERT
Date: 2018.10.25 08:56:02 -04'00'

Jerry Horton
Chief Information Officer

Response to recommendations presented in the Draft OIG Report, "*2018 Audit of the BCFP's Information Security Program*."

Recommendation 1: Strengthen configuration management processes by
a. Remediating configuration-related vulnerabilities in a timely manner
b. Ensuring that optimal resources are allocated to perform vulnerability remediation activities.

Management Response: The Bureau concurs with this recommendation. BCFP currently has policies and procedures that prescribe remediation timelines for configuration-related vulnerabilities identified on BCFP systems. While timelines are clearly defined in existing policies, resource constraints occasionally impact the timely remediation of configuration-related vulnerabilities. Additionally, if the Bureau encounters configuration changes that detrimentally affect applications, we conduct a risk analysis to assess impact and apply compensating controls accordingly. In FY19, the Bureau will ensure that approved compensating controls are fully documented so that configuration-related vulnerabilities are efficiently tracked and mitigated. The Bureau will also work to ensure that adequate resources are prioritized to support configuration-related vulnerability remediation efforts.

Recommendation 2: Develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.

Management Response: The Bureau concurs with this recommendation. Current processes inform end users of necessary patches to agency-issued mobile devices when available. However, installation of the update/patch must be initiated by the end user of the device. In FY 2019, the Bureau is deploying a unified endpoint management solution, which will enable Bureau system administrators to centrally push necessary updates and patches directly to mobile devices without user interaction.

Recommendation 3: Determine whether established processes and procedures for management of privileged user access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.

Management Response: The Bureau concurs with this recommendation. The BCFP has an established process and procedures for management of privileged user access agreements and rules-of-behavior acknowledgment documents. Continuing into FY 2019, the Bureau is implementing a new information technology service management (ITSM) tool that will automate much of the existing processes and integrate with other user account provisioning functions to ensure consistent procedural and technical access controls. Until the tool is implemented, the Bureau will incorporate additional workflow controls to further mature this process. Lastly, the Bureau will ensure that adequate resources are assigned to make changes as needed.

Recommendation 4: Ensure that the Bureau's existing information security continuous monitoring approach is implemented for an internal collaboration tool to appropriately restrict and monitor access.

Management Response: The Bureau concurs with the recommendation. In FY 2018, the Bureau initiated a project to protect unstructured data within the internal collaboration environment. This technology will provide visibility into end-user access to sensitive data and prompt any remediating action. The Bureau will continue to prioritize efforts to fully implement this solution.

Abbreviations

Bureau	Bureau of Consumer Financial Protection
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
DHS	U.S. Department of Homeland Security
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
ICAM	identity, credential, and access management
IG	Inspector General
IT	information technology
ISCM	information security continuous monitoring
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
PIV	personal identity verification
SP 800-39	Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
SP 800-53	Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
SP 800-122	Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*
SP 800-128	Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
SP 800-137	Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

Report Contributors

Khalid Hasan, Senior OIG Manager
Andrew Gibson, OIG Manager
Rebecca Kenyon, Senior IT Auditor
Kaneisha Johnson, IT Auditor
Emily Martin, IT Auditor
Jeff Woodward, IT Auditor
La' Toya Holt, Auditor
Justin Byun, IT Audit Intern
Peter Sheridan, Associate Inspector General for Information Technology

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044