Audit Report
2020-IT-C-021
November 2, 2020

Bureau of Consumer Financial Protection

2020 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, 2020-IT-C-021, November 2, 2020

2020 Audit of the Bureau's Information Security Program

Findings

The Bureau of Consumer Financial Protection's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. For instance, the Bureau's information security continuous monitoring process is effective; the agency integrated metrics on the effectiveness of its process across the organization. Further, the Bureau's incident response process is similarly effective; the agency implemented a new incident ticket system that is more closely integrated with configuration management activities.

Similar to previous years, we identified opportunities for the Bureau to strengthen its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five National Institute of Standards and Technology Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. This year, we identified policy and technology improvements needed to strengthen separation of duties controls in the Bureau's configuration management processes.

We also found that the Bureau has taken sufficient actions to close 4 of the 14 recommendations from our prior FISMA audits that were open at the start of this audit. These 4 recommendations are related to risk management, identity and access management, and incident response. The remaining 10 recommendations, related to risk management, configuration management, identity and access management, data protection and privacy, incident response, and contingency planning, remain open. We will continue to monitor the Bureau's progress in these areas as part of our future FISMA reviews

Recommendation

This report includes one new recommendation designed to strengthen the Bureau's information security program in the area of configuration management. In its response to a draft of our report, the Bureau concurs with our recommendation and outlines actions that have been or will be taken to address it. We will continue to monitor the Bureau's progress in addressing this recommendation as part of future FISMA 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. The U.S. Department of Homeland Security's guidance for FISMA reporting directs inspectors general to evaluate the maturity level (from a low of 1 to a high of 5) of their agencies' information security programs across several areas. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.

Recommendations, 2020-IT-C-021, November 2, 2020

2020 Audit of the Bureau's Information Security Program

Number	Recommendation	Responsible office
1	Ensure that a. change control policies and procedures address separation of duties in the change management life cycle. b. separation of duties is enforced in the Bureau's change control tool.	Office of Technology and Innovation

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

MEMORANDUM

DATE: November 2, 2020

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2020-IT-C-021: *2020 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 (FISMA), which requires each agency inspector general to conduct an annual independent evaluation of the effectiveness of its agency's information security program and practices. As part of our work, we analyzed key FISMA-related data, performed data analytics, and conducted technical testing. We will use the results of this audit to respond to specific questions in the U.S. Department of Homeland Security's *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

We provided you with a draft of our report for review and comment. In your response, you concur with our recommendation and outline actions that have been or will be taken to address our recommendation. We have included your response as appendix C 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: Katherine Sickbert
Tiina Rodrigue
Tannaz Haddadi
Marianne Roth
Kirsten Sutton
Elizabeth Reilly
Dana James
Lauren Hassouni
Anya Veledar
Carlos Villa

Distribution:
Donna Roy, Chief Information Officer and Chief Operating Officer
Martin Michalosky, Chief Administrative Officer
Ren Essene, Chief Data 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 (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 their respective agency, including testing the effectiveness of information security policies, procedures, and practices for select systems.

To support independent evaluation requirements, the U.S. Department of Homeland Security (DHS) publishes FISMA reporting metrics for IGs to respond to on an annual basis. The *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* directs IGs to evaluate the effectiveness of agency information security programs across a variety of attributes grouped into eight security domains.[2] 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* (table 1).[3]

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

[2] U.S. Department of Homeland Security, *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 4.0, April 17, 2020.

[3] The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.

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

Security function	Security function objective	Associated IG FISMA 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 to prevent, limit, or contain the impact of a cybersecurity event.	Configuration management, identity and access management, data protection and privacy, 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 2020 IG FISMA Reporting Metrics*.

As noted in DHS's *FY 2020 IG FISMA Reporting Metrics*, one of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving outcomes that strengthen federal cybersecurity, including their implementation of the administration's priorities and best practices. Two of these priorities include the security of mobile devices and the modernization of the Trusted Internet Connections (TIC) initiative. Specifically, DHS's *FY 2020 CIO FISMA Metrics* includes an additional focus on the security of mobile devices (government-furnished equipment and non-government-furnished equipment), particularly in the areas of mobile device management and enterprise mobility management.[4] In addition, the Office of Management and Budget (OMB) provided updated guidance to federal agencies on the use of TIC capabilities in modern architectures and frameworks such as cloud environments.[5] As such, DHS's *FY 2020 IG FISMA Reporting Metrics* have been updated to gauge the effectiveness of agencies' processes to secure mobile endpoints, employ secure application development processes, and plan for the effective implementation of the security capabilities outlined in OMB's updated TIC guidance.

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 OMB, DHS, and other key stakeholders, developed a maturity model intended to better address and report on the effectiveness of an agency's information

[4] U.S. Department of Homeland Security, *FY 2020 CIO FISMA Metrics*, Version 1, October 2019.

[5] Office of Management and Budget, *Update to the Trusted Internet Connections (TIC) Initiative*, OMB Memorandum M-19-26, September 2019.

security program. The purpose of the maturity model is (1) to summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) to provide transparency to agency chief information officers (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) to help ensure that annual FISMA reviews are consistent across IGs.

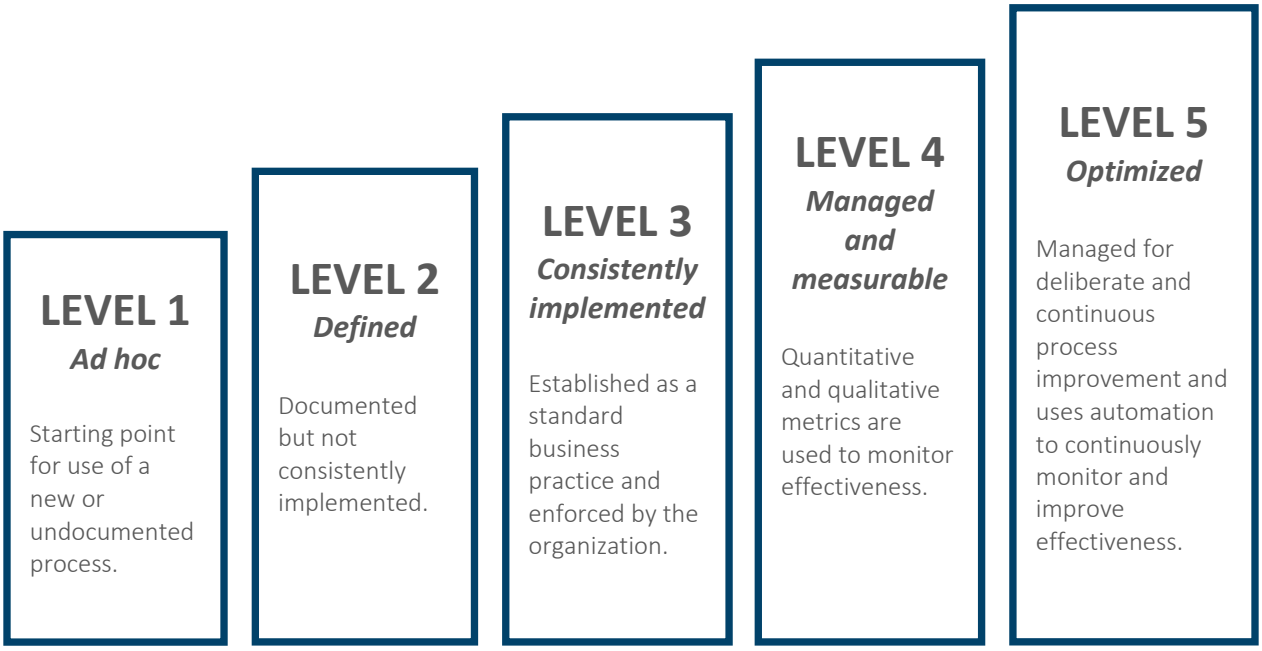
The five levels of the IG FISMA maturity model are

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

The foundational levels (1–3) of the model represent the degree to which policies and procedures are being developed and implemented, and the advanced levels (4–5) capture the extent to which agencies have institutionalized 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 2020 IG FISMA Reporting Metrics*, level 4 (*managed and measurable*) represents an effective level of security.[6] This is the third year that all FISMA security domains will be assessed using the maturity model. Details on the scoring methodology for the maturity model can be found in appendix A.

[6] NIST 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. National Institute of Standards and Technology, *Security and Privacy of Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, updated January 22, 2015.

Figure 1. FISMA Maturity Model Rating Scale

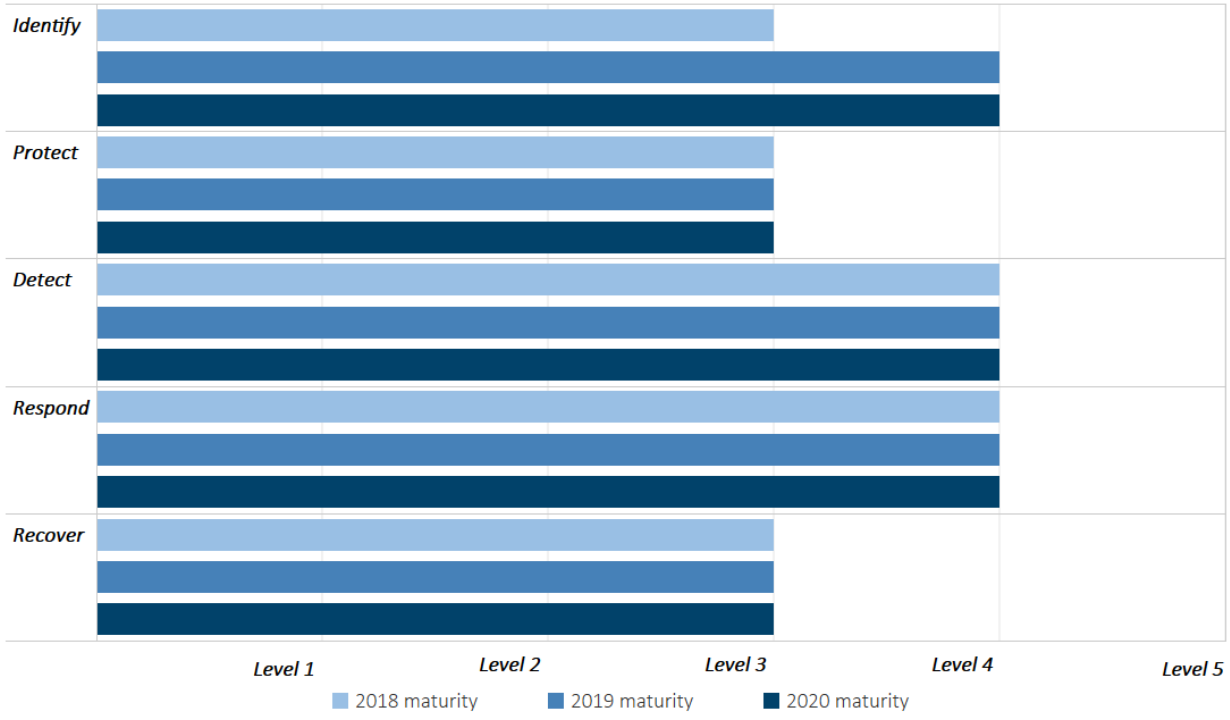


Source: OIG analysis of DHS's *FY 2020 IG FISMA Reporting Metrics.*

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

The Bureau's overall information security program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 2).[7] For instance, within the *identify* function, the Bureau strengthened its asset management program by employing automation to track the life cycle of its hardware assets. Similar to previous years, we identified opportunities for the Bureau to strengthen its information security program in FISMA domains across all five NIST Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. This year, we identified policy and technology improvements needed to strengthen separation of duties controls in the Bureau's configuration management processes, and our report includes 1 new recommendation in this area. In addition, we are closing 4 recommendations made during our previous years' FISMA audits and keeping 10 recommendations open.

Figure 2. Maturity of the Bureau's Information Security Program, by Security Function, 2018–2020



Source: OIG analysis.

[7] To determine the maturity of the Bureau's information security program, we used the scoring methodology outlined in DHS's *FY 2020 IG FISMA Reporting Metrics*. Appendix A provides additional details on the scoring methodology.

Identify

The objective of the *identify* function in NIST's 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. Examples of the areas in this security function, as outlined in DHS's *FY 2020 IG FISMA Reporting Metrics*, that we assessed include the Bureau's processes for enterprise risk management (ERM); the development and implementation of an enterprise architecture; asset management, including mobile device management; and the use of plans of action and milestones to manage the remediation of security weaknesses.

Risk Management

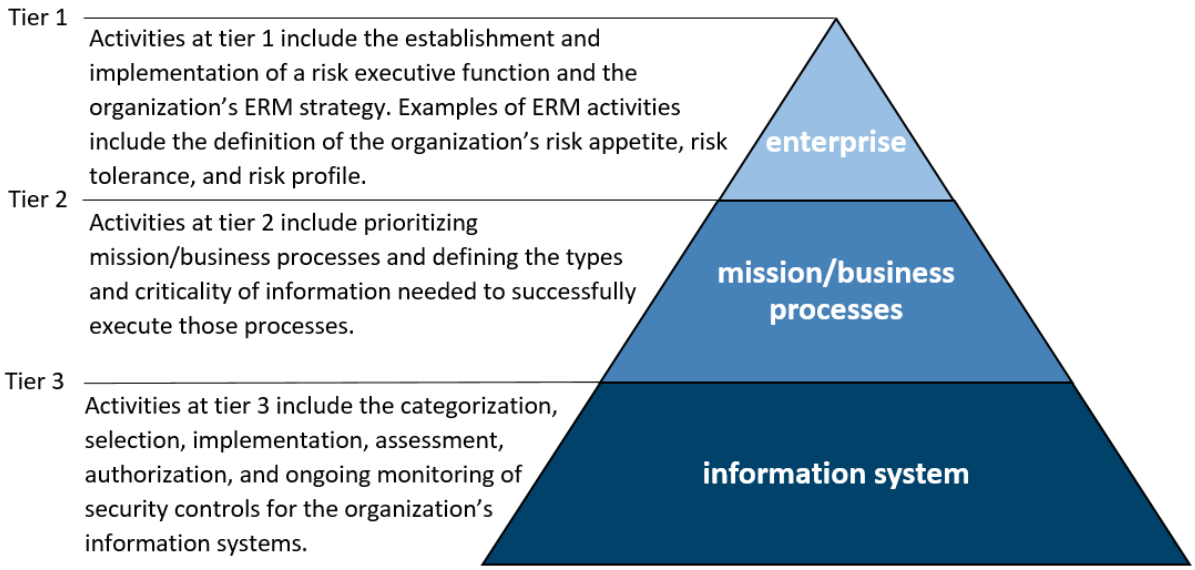
FISMA requires federal agencies to provide information security protections commensurate with their risk environment and to ensure that information security management processes are integrated with strategic, operational, and budgetary planning processes. *Risk management* refers to the program and supporting processes used to manage risk to organizational operations, assets, and individuals and is a holistic activity that affects every aspect of the organization. Federal guidance notes the importance of ERM, which is an effective agencywide approach to addressing the full spectrum of the organization's external and internal risks. Through ERM, agencies understand the combined effect of risks as an interrelated portfolio, rather than address risks within silos. Federal guidance also emphasizes that an effective ERM program promotes a common understanding for recognizing and describing potential risks, such as cybersecurity, strategic, market, legal, and reputational risks that can affect the agency's mission.[8]

The relationship between cybersecurity risk management and ERM is further outlined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, which states that effective risk management involves the integration of activities at the enterprise, mission and business process, and information system levels.[9] The risk management process should be carried out across these three tiers, with the overall objective of continuous improvement in the organization's risk-related activities and effective communication among stakeholders (figure 3). The risk management guidance described in this special publication is complementary to and should be used as part of a more comprehensive ERM program.

[8] According to OMB Memorandum M-17-25, *cybersecurity risk management* refers to the full range of activities undertaken to protect information technology and data from unauthorized access and other cyberthreats; to maintain awareness of cyberthreats; to detect anomalies and incidents adversely affecting information technology and data; and to mitigate the effect of, respond to, and recover from incidents. Office of Management and Budget, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, OMB Memorandum M-17-25, May 9, 2018.

[9] National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39, March 1, 2011.

Figure 3. The Three Tiers of Risk Management

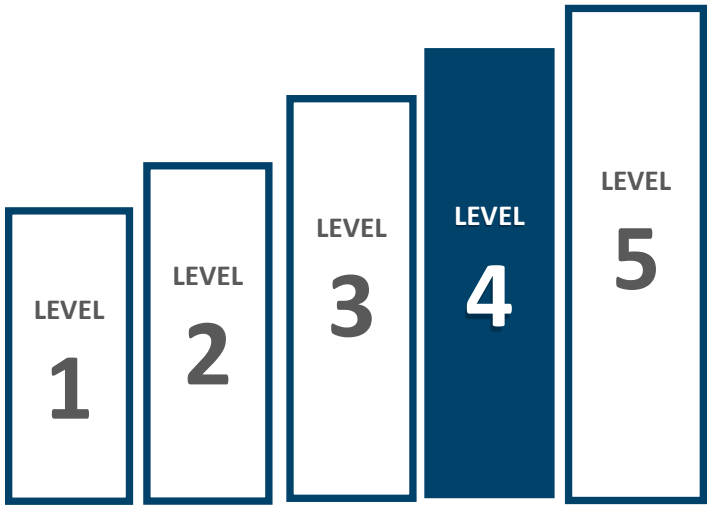


Source: NIST Special Publication 800-39.

Current Agency Maturity

As in 2019, we found that the Bureau's risk management program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 4). For example, the Bureau continues to ensure that its information systems are subject to the monitoring processes defined within its information security continuous monitoring (ISCM) program. In addition, the Bureau continues to maintain qualitative and quantitative performance measures related to its plans of action and milestones process.

Figure 4. Risk Management, Level 4 (*Managed and Measurable*)



Source: OIG analysis.

This year, we found that the Bureau has continued to make progress in maturing its enterprise and cybersecurity risk management programs in the areas of risk appetite, risk tolerance, and security assessment and authorization (SA&A); however, our recommendations in these areas from prior FISMA reports remain open.[10] Specifically, we noted the following:

[10] Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*, OIG Report 2016-IT-C-012, November 10, 2016; and Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*, OIG Report 2019-IT-C-015, October 31, 2019.

- The Bureau is in the process of finalizing its risk appetite statement and risk tolerance levels, which agency officials informed us are projected to be completed by the fourth quarter of 2020.

- The Bureau is working toward implementing processes that will prohibit future instances of systems being placed into production without the completion of SA&A activities. Further, this year the Bureau updated its *Risk Management Handbook*, which describes an approach for the Bureau to integrate key cybersecurity activities during all phases of the system life cycle: definition, design, development, assessment, deployment, operation, maintenance, and disposal of the system.[11]

The status of prior FISMA recommendations made in these areas is in appendix B. We believe that addressing these open recommendations will help the Bureau mature its information security program. For instance, the finalization of the Bureau's risk appetite statement and tolerance levels could help guide and direct the mitigation of risks identified through the agency's continuous monitoring processes. We will continue to follow up on the Bureau's efforts in these areas as part of our future FISMA reviews.

Protect

The objective of the *protect* function in NIST's Cybersecurity Framework is to develop and implement safeguards to secure information systems. This function supports the ability to prevent, limit, or contain the effect of a cybersecurity event through applicable configuration management, identity and access management, data protection and privacy, and security training processes. The *protect* function has four security domains with associated components that IGs are required to assess (table 2).

Table 2. *Protect* Function Security Domains and Selected Components

Security domains	Examples of components assessed by IGs
Configuration management	Configuration management plans, configuration settings, flaw remediation, and change control
Identity and access management	Identity, credential, and access management strategy; access agreements; and background investigations
Data protection and privacy	Security controls for exfiltration, privacy security controls, and privacy awareness training
Security training	Assessment of knowledge, skills, and abilities; security awareness; and specialized security training

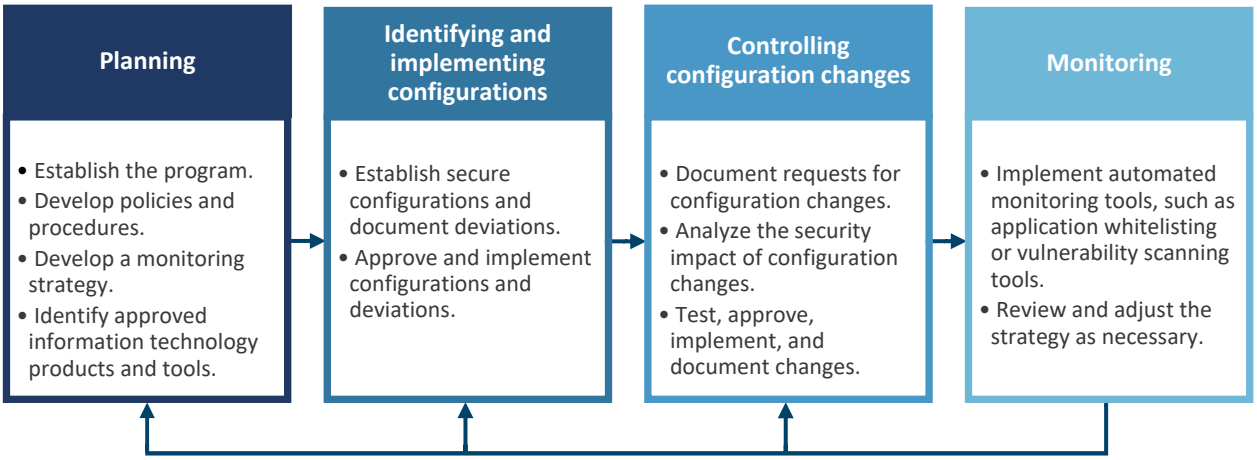
Source: U.S. Department of Homeland Security, *FY 2020 IG FISMA Reporting Metrics*.

[11] The Bureau finalized its *Risk Management Handbook* at end of our fieldwork. We plan to assess the handbook's effectiveness as part of our future FISMA reviews.

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.[12] 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 5).

Figure 5. Security-Focused Configuration Management Phases



Source: NIST Special Publication 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 the 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 cyberattack.

With respect to patch management, NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53), states that organizations should install security-relevant software and firmware updates within organization-defined time frames and incorporate flaw remediation into configuration management processes.[13] In addition, NIST Special

[12] National Institute of Standards and Technology, *Guide for Security-Focused Configuration Management of Information Systems*, Special Publication 800-128, updated October 10, 2019.

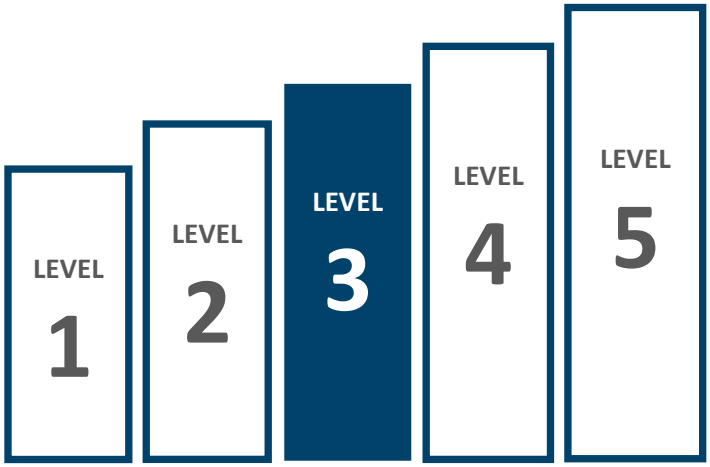
[13] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, January 2015.

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.[14] It also states that enterprise mobile device management software can be used to keep mobile device software updated and to restrict access if the device's operating system is not up to date.

Current Agency Maturity

As in 2019, we found that the Bureau's configuration management program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level (figure 6). 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. In addition, this year the Bureau centralized multiple configuration management processes, such as for hardware and software inventory and change requests, into a single tool. Bureau officials also notified us that the agency's configuration management database has been integrated into this tool, enabling better tracking of changes.

Figure 6. Configuration Management, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

Although the Bureau has strengthened several configuration management–related processes, several of our recommendations in this area from prior FISMA reports remain open.[15] Specifically, we noted the following:

- The Bureau is in the process of selecting and implementing a database-level vulnerability scanning product. Officials noted that they have selected a product and are working to obtain budgetary approval to acquire and implement the tool in the next fiscal year.

- The Bureau has implemented process and technological changes that have reduced the number of critical and high-risk vulnerabilities open beyond required time frames. Specifically, the Bureau now requires system owners and cybersecurity team members to meet on a weekly basis to discuss open vulnerabilities, and it created dashboards that system owners can access that show

[14] National Institute of Standards and Technology, *Guide to Enterprise Patch Management Technologies*, Special Publication 800-40, Revision 3, July 2013.

[15] 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, *2018 Audit of the Bureau's Information Security Program*, OIG Report 2018-IT-C-018, October 31, 2018.

the open vulnerabilities in real time. However, further improvements are needed to ensure that critical and high-risk vulnerabilities are remediated in a timely manner.

- The Bureau is in the process of implementing a new mobile device management system that will provide it with the ability to enforce current patch levels for agency-issued mobile phones. Bureau officials informed us that all agency-issued mobile phones will be moved to the new system. At that time, the Bureau plans to enforce current patch levels for its mobile phones.

The status of prior FISMA recommendations made in these areas is in appendix B. We believe that addressing these recommendations will help the Bureau mature its configuration management program. We will continue to follow up on the Bureau's efforts in these areas as part of our future FISMA reviews.

This year, we also found that the Bureau lacks policy and technological restrictions to ensure adequate separation of duties within its change control processes. Specifically, we found that the Bureau's change request policies and procedures do not address restrictions concerning separation of duties for the opening and closing of tickets. Further, the tool used for creating, monitoring, and closing change request tickets allows all change requests to be opened and closed by the same person. Bureau officials stated that the cause for these issues is that they have yet to finalize their process flows and documentation for the new change request tool; in the interim, they have been speaking with staff individually to ensure they are aware that the same person opening and closing a ticket is prohibited. Our sampling of 27 change control tickets in the Bureau's new change request tool revealed that 3 change requests were opened and closed by the same person. Bureau officials notified us that they are in the process of changing configurations in the tool to restrict the ability of users to close change requests that they themselves opened.

NIST SP 800-53 states that separation of duties includes, for example, conducting information support functions (for example, system management, programming, configuration management, quality assurance and testing, and network security) with different individuals. Further, NIST SP 800-128 states that in order to maintain adequate separation of duties, users should not be given the authority to unilaterally propose and approve changes to the configuration of a system (excluding changes identified in procedures as being exempt from security-focused configuration management). By updating policy requirements to explicitly address the separation of duties in the change control process and making necessary technological updates, the Bureau will have greater assurance that changes do not introduce unnecessary risks into the agency's information technology (IT) environment.

Recommendation

We recommend that the CIO

1. Ensure that
    a. change control policies and procedures address separation of duties in the change management life cycle.
    b. separation of duties is enforced in the Bureau's change control tool.

Management Response

The CIO concurs with the recommendation. The CIO notes that the Bureau's Enterprise Architecture team has received approvals to enhance the functionality of the agency's workflow within its change management tool to restrict who may close change management tickets. This update will ensure that the necessary approvals are obtained and that the change management process is followed. Further, the CIO notes that the enhancement in functionality is in keeping with separation of duties because only a member of the Change Management team may record approvals and close the change request after all applicable steps, reviews, and information are completed.

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.

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 7).

Figure 7. ICAM Conceptual Design

Source: CIO Council, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.*

Effective identity and access management is a key control area for managing the risk from insider threats, and FISMA requires agencies to implement controls to preserve authorized restrictions on access and disclosure. 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 CIO Council has published *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance* to provide the government with a common framework and implementation guidance to plan and execute ICAM programs.[16] Another key component of effective identity and access management is controlling the use of privileged accounts with

[16] CIO Council, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Version 2.0, December 2, 2011.

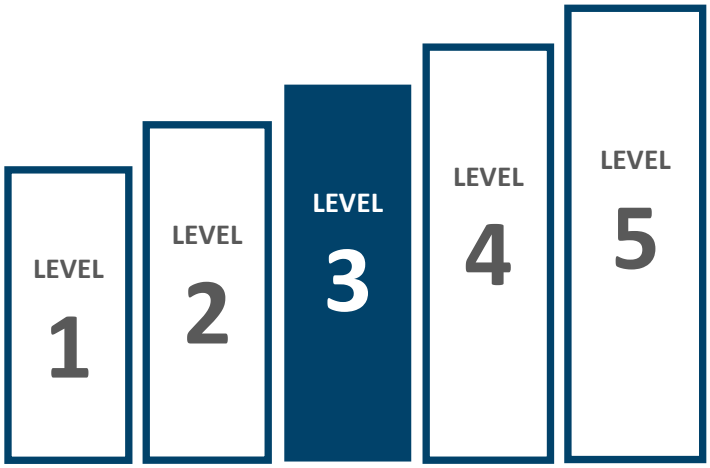
elevated rights that provide broad, direct access to information systems. NIST SP 800-53 emphasizes the importance of tracking and controlling access privileges and ensuring that these privileges are periodically reviewed and adjusted.

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 management of privileged accounts, the Bureau's policies and procedures require privileged users to annually resubmit their signed and approved user-access agreements and rules-of-behavior forms or their privileged access will be revoked.

Current Agency Maturity

As in 2019, we found that the Bureau's identity and access management program is operating at a level-3 (*consistently implemented*) maturity (figure 8). For instance, the Bureau has developed an ICAM roadmap that defines an implementation strategy and is on track to meet milestones. The roadmap also aligns with *FICAM Roadmap and Guidance* and Continuous Diagnostics and Mitigation requirements and incorporates applicable federal policies, standards, playbooks, and guidelines. The roadmap notes that the Bureau will reach its desired state for identify and access management before the end of fiscal year 2022.

Figure 8. Identity and Access Management, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

This year, we found that the Bureau is continuing to mature its information security processes related to multifactor authentication and maintenance of user-access agreements and rules-of-behavior forms for individuals with privileged access, and recommendations in these areas from prior FISMA reports remain open.[17] Specifically, we noted the following:

- In May 2020, the Bureau initiated a project to implement a privileged account management tool that will require multifactor authentication for privileged access. Further, according to Bureau officials, the agency procured a tool that will require multifactor authentication for nonprivileged users through the use of derived credentials. The Bureau's ICAM roadmap identifies that these tools will be implemented by the third quarter of fiscal year 2021.

[17] Office of Inspector General, *2017 Audit of the CFPB's Information Security Program*, OIG Report 2017-IT-C-019, October 31, 2017; Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*; and Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*.

- The Bureau plans to use a new configuration management tool to better manage user-access agreements and privileged user rules-of-behavior forms. This year, our sampling of user-access agreements and rules-of-behavior forms for privileged and nonprivileged users of two systems revealed discrepancies similar to those we reported on in the past 2 years, such as missing and outdated documentation. Officials stated that moving the management of this documentation into the new tool may remediate these ongoing issues.

The status of prior FISMA recommendations made in this area is in appendix B. We believe that addressing these recommendations will help the Bureau mature its identity and access management program. We will continue to follow up on the Bureau's efforts in these areas as part of our future FISMA reviews.

Data Protection and Privacy

Data protection and privacy refers to a collection of activities focused on preserving authorized restrictions on information access and protecting personal privacy and proprietary information. 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, federal guidance[18] requires covered federal agencies to develop, implement, and maintain agencywide privacy programs that play a key role in PII information security and that implement the NIST Risk Management Framework.[19] While 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 covered agency heads to designate a senior agency official for privacy who has agencywide responsibility and accountability for the agency's privacy program.[20]

NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, notes the importance of identifying all PII residing in the organization or under the control of a third party on behalf of the organization.[21] Further, this special publication 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).

[18] Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130, July 28, 2016.

[19] NIST has developed a risk management framework and associated guidelines to provide a structured and flexible process for managing security and privacy risk for federal information and information systems that includes security categorization, control selection, implementation and assessment, authorization, and continuous monitoring. National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2, December 2018.

[20] Exec. Order No. 13719 (February 9, 2016).

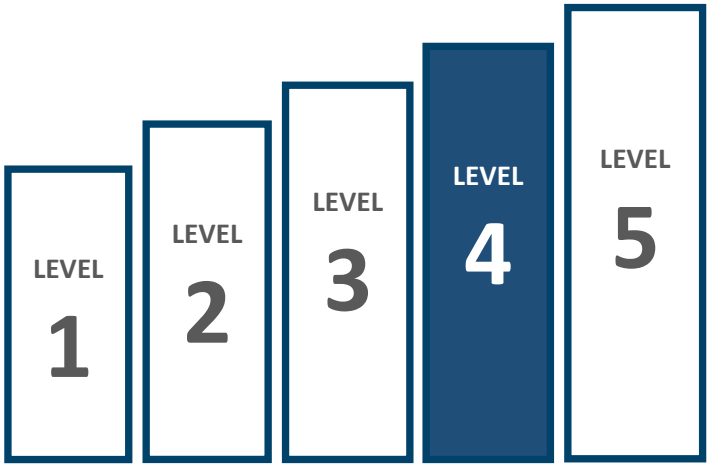
[21] National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Publication 800-122, April 6, 2010.

To meet its mission of regulating the offerings and provisions of consumer financial products and services under federal consumer financial laws, the Bureau collects sensitive PII.[22] 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 Agency Maturity

We found that the Bureau has matured its data protection and privacy program from a level-3 maturity in 2019 to a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 9). For example, the Bureau has established a *Data Breach Response Plan* and established metrics to measure the plan's effectiveness. The Bureau has also defined, communicated, and implemented its privacy awareness and role-based training programs and tailored them to its environment.

Figure 9. Data Protection and Privacy, Level 4 (*Managed and Measurable*)



Source: OIG analysis.

The Bureau can continue to mature its data protection and privacy program in the area of data exfiltration controls, which we previously identified as an issue for the Bureau. Specifically, in our 2019 FISMA report we identified that the Bureau could improve its data exfiltration controls to better ensure the protection of sensitive agency data. We found that a technology the Bureau was using to monitor and control data exfiltration was not consistently implemented across the agency's IT environment.[23] For instance, this technology was not blocking access to known internet storage sites and was not deployed across the Bureau's entire network. This year, we found that although the Bureau has begun integrating its data loss protection (DLP) tool and its Security Information Event Management system, it has opportunities to consistently implement the tool across its network. As such, we are leaving our 2019 FISMA audit recommendation in this area open and will continue to follow up on the Bureau's efforts as a part of our future FISMA audits.

We also found that access controls were not appropriately set in the Bureau's internal collaboration tool for specific sites, which affected one agency division and resulted in sensitive information (including PII) being made available to users who did not have a valid need to know. We communicated the details of this issue to the Bureau in a separate, restricted memorandum. After we notified the Bureau of these issues, it took immediate actions to restrict access. Bureau officials stated that they reviewed the logs associated with the sites and verified that there was no inappropriate access and that permissions had

[22] 12 U.S.C. §§ 5491(a).

[23] Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*.

been remediated. We will continue to monitor the Bureau's progress to strengthen controls for its internal collaboration tools as part of our future FISMA reviews.

Security Training

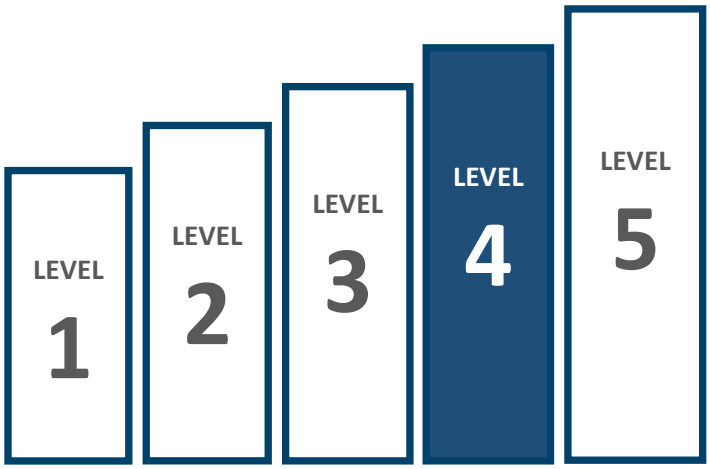
FISMA requires agencies to develop an information security program that provides security awareness training to personnel, including contractors, who support the operations and assets of the organization, as well as role-based training for individuals with significant information security responsibilities. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, states that in general, people are one of the weakest links in securing agency systems and networks.[24] As such, a robust, enterprisewide security awareness and training program is paramount to ensure that people understand their IT security responsibilities and organizational policies and know how to properly use and protect the IT resources entrusted to them.

In accordance with FISMA requirements, the Bureau's *Cybersecurity Awareness and Training Process* document states that all employees and contractors with access to agency information systems must receive security awareness training before being permitted access to the Bureau's 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 attendance be maintained.

Current Agency Maturity

As in 2019, we found that the Bureau's security training program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 10). For example, the Bureau has completed a knowledge, skills, and abilities assessment of its employees. In addition, the Bureau has updated its phishing program to reflect COVID-19 pandemic considerations and is providing its workforce with security-related tips specific to the pandemic.

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



Source: OIG analysis.

Although we do not have any open or new recommendations regarding the Bureau's security training program, we believe that the Bureau can further mature its processes in this area. Specifically, we found that the Bureau can improve its security training program by updating its policies and procedures on a timelier basis. Additionally, the Bureau can use targeted phishing exercises and obtain metrics or results on the effectiveness of its security training offerings to gauge how well it is aligning to NIST's *National Initiative*

[24] National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program*, Special Publication 800-50, October 1, 2003.

for Cyber Education (NICE) Workforce Framework.[25] Completing these activities could help the Bureau mature its security training program and fully institutionalize a process of continuous improvement that incorporates advanced security practices. We will continue to monitor the Bureau's progress in maturing its security training program as part of our future FISMA reviews.

Detect

The objective of the *detect* function in NIST's 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 operational environment, maintain knowledge of threats, and ensure security control effectiveness. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2020 IG FISMA Reporting Metrics*, that we assessed include the Bureau's progress to develop and implement an ISCM strategy, to perform ongoing system authorizations, and to use ISCM-related performance measures.

Information Security Continuous Monitoring

ISCM refers to the process of maintaining an 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 (ISCM) for Federal Information Systems and Organizations* (SP 800-137).[26] SP 800-137 states 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 an ISCM strategy is defined, SP 800-137 states 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 (1) it sufficiently supports the organization's operation within acceptable risk tolerance levels, (2) metrics remain relevant, and (3) data are current and complete. In 2020, NIST published Special Publication 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, which can be used to guide the development of an ISCM strategy.[27] This special publication states that creating and using an ISCM program assessment can help guide the development of an ISCM strategy and reduce the overall risk to organizations by identifying gaps in an ISCM program.

---

[25] National Institute of Standards and Technology, *National Initiative for Cyber Education (NICE) Workforce Framework*, Special Publication 800-181, August 7, 2017.

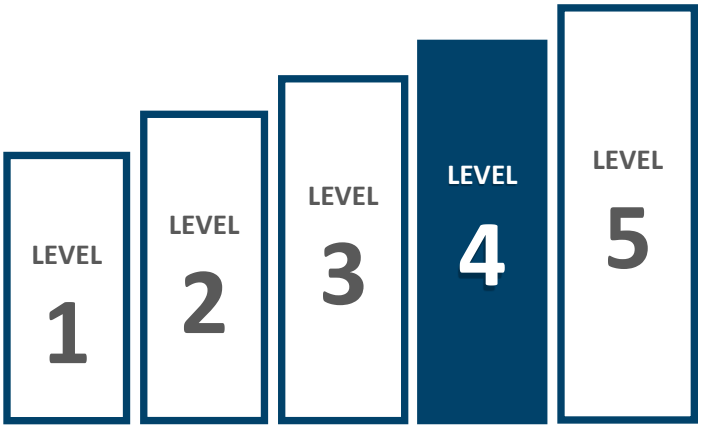
[26] National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, Special Publication 800-137, September 30, 2011.

[27] National Institute of Standards and Technology, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, Special Publication 800-137A, May 21, 2020.

Current Agency Maturity

As in 2019, we found that the Bureau's ISCM program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 11). For instance, the Bureau has defined and communicated roles and responsibilities for ISCM stakeholders and identified skill gaps and training needs for ISCM staff. In addition, the Bureau has integrated metrics on the effectiveness of its ISCM program across the organization.

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



Source: OIG analysis.

Although we do not have any open or new recommendations for the Bureau's ISCM program, we believe that taking steps to address our open recommendation on defining a risk appetite statement and associated risk tolerance levels could have an effect on the maturity of the ISCM program. For instance, the Bureau is finalizing its risk appetite statement and tolerance levels, and these decisions may affect the frequency of controls monitoring and risk remediation activities. In addition, the Bureau has recently updated its *Risk Management Handbook*.[28] According to Bureau officials, the handbook documents and updates the Bureau's continuous monitoring strategy. We noted, however, that the handbook does not address how ISCM processes are integrated at the enterprise level, nor does it address the management of enterprise-level risks. We will continue to monitor the Bureau's progress in maturing its ISCM program and integrating it with ERM processes as part of our future FISMA reviews.

Respond

The objective of the *respond* function in NIST's 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. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2020 IG FISMA Reporting Metrics*, that we assessed include the Bureau's incident detection, analysis, handling, and reporting processes.

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 states that an incident response process consists of four main phases: preparation; detection and

[28] The Bureau finalized its *Risk Management Handbook* toward the end of the completion of our fieldwork. As such, we did not test its effectiveness as part of our audit.

analysis; containment, eradication, and recovery; and postincident activity (table 3).[29] It further states 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 3. 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.

The Bureau's incident response policies and procedures address requirements and processes for incident detection, response, and reporting of information security incidents related to agency data and resources. The policies and 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 on incident response, including reporting incidents to the United States Computer Emergency Readiness Team (US-CERT) within an hour as required by the *US-CERT Federal Incident Notification Guidelines*.[30]

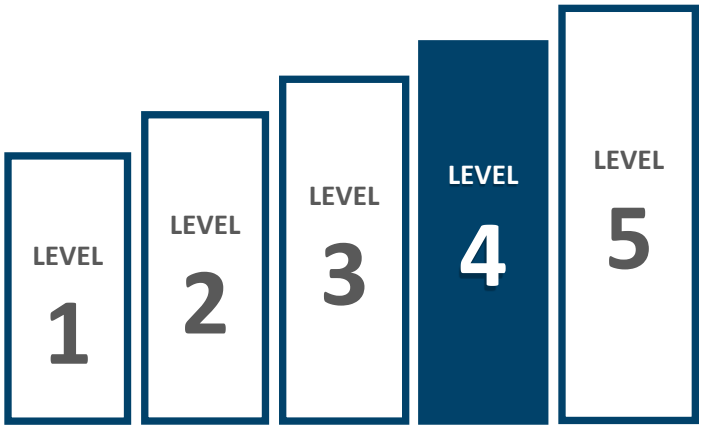
[29] National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, Revision 2, August 6, 2012.

[30] U.S. Department of Homeland Security, *US-CERT Federal Incident Notification Guidelines*, April 1, 2017.

Current Agency Maturity

As in 2019, we found that the Bureau's incident response program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 12). For instance, the agency has implemented a new incident ticketing system that is more closely integrated with configuration management activities. In addition, the agency continues to capture and assess incident response performance measures. For example, the Bureau tracks the timeliness of incident reporting to US-CERT. The Bureau's metrics in this area show that qualifying incidents are being reported to US-CERT within 10 minutes.

Figure 12. Incident Response, Level 4 (*Managed and Measurable*)



Source: OIG analysis.

This year, we analyzed several quarters' worth of security incident tickets and found that the Bureau's resources for incident response are deployed in a risk-based manner. Further, we found that the Bureau intakes and analyzes alerts, advisories, and indicators of compromise from DHS. We also identified a marked improvement in the categorization of incident tickets, which resulted in our closing of a 2019 recommendation in this area. The status of our prior FISMA recommendations is in appendix B.

Although we have no new or open recommendations this year regarding the Bureau's incident response program, we found that the Bureau can mature specific processes in this area. For example, prior to incident ticket closure, the Bureau uses a peer review process to ensure the quality and accuracy of information contained in the ticket. We found that the Bureau has a backlog of over 700 security tickets that have yet to undergo peer review. Bureau officials stated that this backlog resulted from an 80 percent increase in suspicious email tickets created since the start of 2020. Bureau officials also stated that they are in the process of peer reviewing these tickets, which were made in a ticket system that has since been replaced, and that they have also streamlined the peer review process. Because the Bureau has transitioned to a new incident ticket system that offers greater functionality, has streamlined its peer review process, and is taking steps to remediate the backlog of tickets, we are not making a recommendation in this area at this time. We will continue to follow up on the Bureau's actions in this area as part of future FISMA reviews.

Recover

The objective of the *recover* function in NIST's 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. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2020 IG FISMA Reporting Metrics*, that we assessed include the Bureau's processes for developing and testing information system contingency plans and the management of contingency planning considerations related to the agency's information and communications technology (ICT) supply chain.

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* (SP 800-34), provides best practices for information system contingency planning.[31]

SP 800-34 states that conducting a business impact analysis (BIA) is a key component of the information system contingency planning process and enables an organization to characterize system components, supported mission and business processes, and interdependencies. NIST SP 800-34 further states that continuity of operations functions are subject to a process-focused BIA, while federal information systems are subject to a system-focused BIA. A system-level BIA consists of three main components and can leverage the information contained in the process-focused BIA: (1) determination of mission and business processes supported by the system and associated recovery capability, (2) identification of resource requirements, and (3) identification of recovery priorities for system resources.

Another key component of an effective contingency planning program is the consideration of risk from an organization's ICT supply chain. NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, highlights ICT supply chain concerns associated with contingency planning, including alternative suppliers of system components and services, denial-of-service attacks to the supply chain, and alternative delivery routes for critical system components.[32] In addition, in December 2018 the SECURE Technology Act was passed to strengthen agency supply chain risk management practices. The act establishes a Federal Acquisition Security Council to provide agencies with guidance related to mitigating supply chain risks in IT procurement and to establish criteria for determining which types of products pose supply chain security risks to the federal government.[33] The importance of supply chain risk management is also highlighted by its inclusion and enhanced focus in the recent update to the NIST Cybersecurity Framework. For example, with respect to contingency planning, the framework states that response and recovery planning and testing should be conducted with suppliers and third-party providers.

[31] National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34, Revision 1, updated November 11, 2010.

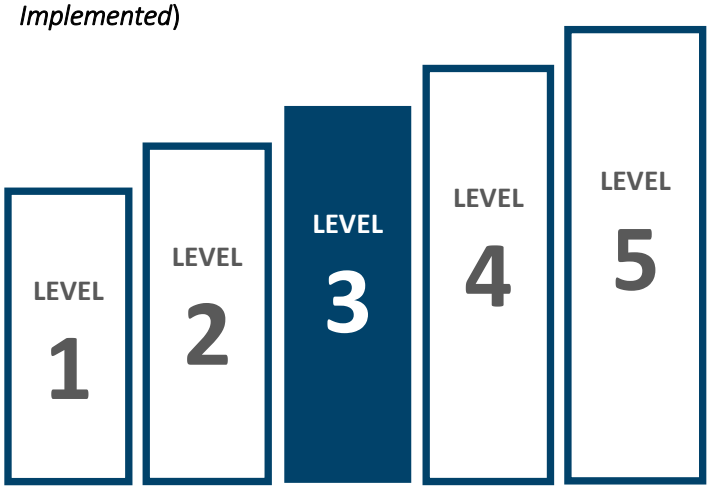
[32] National Institute of Standards and Technology, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Special Publication 800-161, April 8, 2015. The guidance and controls in this special publication are recommended for use with high-impact systems according to Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*. However, according to NIST, because of interdependencies and individual needs, agencies may choose to apply the guidance to systems at a lower impact level or to specific system components.

[33] At the conclusion of our fieldwork, the Federal Acquisition Security Council had not yet issued guidance related to mitigation of ICT supply chain risks.

Current Agency Maturity

As in 2019, we found that the Bureau's contingency planning program is continuing to operate at a level-3 (*consistently implemented*) maturity (figure 13). Specifically, the Bureau has documented its roles and responsibilities for contingency in the Bureau's Continuity of Operations Plan. Additionally, the Bureau continues to implement its backup and storage processes in accordance with its policies and procedures.

Figure 13. Contingency Planning, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

In our 2019 FISMA audit report, we recommended that the CIO ensure that system-level BIAs are conducted and that the results are incorporated into the Bureau's contingency planning strategy and processes.[34] This year, we found that the Bureau has completed BIAs for some, but not all, systems on its FISMA inventory. Completing system-level BIAs will ensure that the Bureau is able to effectively identify critical services within each system and adjust contingency planning priorities and resources as appropriate. As such, we are leaving our 2019 FISMA audit recommendation in this area open and will continue to follow up on the Bureau's efforts as a part of our future FISMA reviews.

Although we are not issuing new recommendations for the Bureau's contingency planning program, we believe that the agency should continue to monitor, and incorporate into its contingency planning program as appropriate, new ICT supply chain guidance issued by the Federal Acquisition Security Council. We will continue to monitor the Bureau's efforts to mature its contingency planning program as part of our future FISMA reviews.

[34] Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*.

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 2020 IG 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 analyzed security policies, procedures, and documentation. In addition, we

- interviewed Bureau management and staff
- performed vulnerability scanning at the network, operating system, and database levels for select systems[35]
- observed and tested specific security processes and controls
- assessed access controls for specific sites in the Bureau's collaboration tool
- performed data analytics to support our effectiveness conclusions for multiple metrics, including those related to plans of action and milestones, security and privacy incidents, and configuration change control tickets

To rate the maturity of the Bureau's information security program and functional areas, we used the scoring methodology defined in DHS's *FY 2020 IG 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 2020 to September 2020. 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.

[35] The detailed results of this testing will be transmitted to the Bureau in a separate, restricted memorandum because of the sensitive nature of the information.

Appendix B: Status of Prior FISMA Recommendations

As part of our 2020 FISMA audit, we reviewed the actions taken by the Bureau to address outstanding recommendations from our prior years' FISMA audits. Below is a summary of the status of the 14 recommendations that were open at the start of our 2020 FISMA audit (table B-1). Based on corrective actions taken by the Bureau, we are closing 4 recommendations related to risk management, identity and access management, and incident response. The remaining 10 recommendations, which are related to risk management, configuration management, identity and access management, data protection and privacy, incident response, and contingency planning, remain open. We will update the status of these recommendations in our spring 2021 semiannual report to Congress, and we will continue to monitor the Bureau's progress in addressing our open recommendations as part of our future FISMA reviews.

Table B-1. Status of 2014–2019 FISMA Recommendations That Were Open as of the Start of Our Fieldwork, by Security Domain

Year		Recommendation	Status	Explanation
Risk management				
2016	1	We recommend that the CIO, in coordination with the chief operating officer, 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 DLP.	Closed	The Bureau has developed an Insider Threat Communication Plan and Charter and an Insider Threat Hub. Further, the Bureau has implemented a DLP tool; we will continue to monitor the agency's progress in fully integrating the tool with its incident response processes. In addition, within the data protection and privacy area, we have an open recommendation related to the coverage of the Bureau's DLP tool.
2017	1	We recommend 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 continues to make progress in establishing and implementing its ERM program, it has not yet finalized its risk appetite statement or risk tolerance levels.

Year		Recommendation	Status	Explanation
2019	1	We recommend that the chief operating officer, the chief data officer, and the CIO determine which components of a high-value asset (HVA) program are applicable to the Bureau and ensure the implementation of a governance structure and HVA-specific baselines and planning activities, as appropriate.	Closed	The Bureau has determined that it does not have any systems that meet the definition and requirements of an HVA. Bureau officials notified us that they will continue to assess their systems for HVA applicability.
2019	2	We recommend that the CIO ensure that established SA&A processes are performed prior to the deployment of all cloud systems used by the Bureau.	Open	We found three instances in which the Bureau had placed systems into production prior to completing its SA&A processes.
Configuration management				
2014	3	We recommend 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 and is in the process of doing so for its databases.
2018	1	We recommend that the CIO strengthen configuration management processes by (a) remediating configuration-related vulnerabilities in a timely manner and (b) ensuring that optimal resources are allocated to perform vulnerability remediation activities.	Open	The Bureau has implemented process and technological changes that have significantly reduced the number of critical and high-risk vulnerabilities that remain open past required dates. However, we continue to identify, as does the Bureau's internal vulnerability scanning, that the agency is not timely remediating numerous critical or high-risk vulnerabilities.
2018	2	We recommend that the CIO develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.	Open	The Bureau is in the process of implementing a new mobile device management system, which will provide the capability to enforce current patch levels for agency-issued mobile phones.

Year		Recommendation	Status	Explanation
Identity and access management				
2017	2	We recommend 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 has begun the process for implementing multifactor authentication for privileged and nonprivileged users. The Bureau plans to have this process completed by the third quarter of fiscal year 2021.
2018	3	We recommend that the CIO 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.	Open	The Bureau is not consistently following its policies and procedures to ensure that user-access agreements and rules-of-behavior forms are completed prior to access being granted to systems. In sampling user-access agreements and rules-of-behavior forms for privileged users of two systems, we identified discrepancies similar to those reported over the past 2 years, such as missing and outdated documentation.
2019	3	We recommend that the CIO ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonprivileged users.	Open	The Bureau is not consistently following its policies and procedures to ensure that user-access agreements and rules-of-behavior forms are completed prior to access being granted to systems. In sampling user-access agreements and rules-of-behavior forms for nonprivileged users of two systems, we identified discrepancies similar to those reported over the past 2 years, such as missing and outdated documentation.
2019	4	We recommend that the chief administrative officer conduct a comprehensive, risk-based review to determine the optimal resources and process for prioritizing the review and adjudication of background investigations.	Closed	The Bureau completed an internal review that identified the need for more resources to prioritize and adjudicate background investigations. As of August 2020, the Bureau reported that there were 20 cases for which adjudication decisions were past 90 days. This is a significant decrease from the 300 cases we identified in our 2019 FISMA review.

Year		Recommendation	Status	Explanation
Data protection and privacy				
2019	5	We recommend that the CIO perform a risk assessment to determine (a) the optimal deployment of the Bureau's technology for monitoring and controlling data exfiltration to all network access points and (b) appropriate access to internet storage sites.	Open	The Bureau has not yet completed its risk assessment to determine the optimal deployment of its technology for monitoring and controlling data exfiltration.
Incident response				
2019	6	We recommend that the CIO and the chief data officer ensure that data captured in security and privacy incident processes and tickets are accurate, consistent, and of high quality.	Closed	We performed data analytics on a sample of security and privacy incident tickets and found that the Bureau has made improvements in this area.
Contingency planning				
2019	7	We recommend that the CIO ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.	Open	The Bureau has not completed system-level BIAs for all the systems on its FISMA inventory.

Source: OIG analysis.

Appendix C: Management Response

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

October 23, 2020

Mr. Peter Sheridan
Associate Inspector General for Information Technology
Board of Governors of the Federal Reserve System &
Bureau of Consumer Financial Protection
20th and Constitution Avenue 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 *2020 Audit of the Bureau's Information Security Program*. We are pleased that you found the Bureau's information security program is operating at an overall Level-4 (*Managed and Measurable*) maturity based on the OIG Federal Information Security Modernization Act of 2014 (FISMA) maturity model. In Fiscal Year (FY) 2021, the Bureau will continue to enhance its processes and technologies to continue to raise its overall maturity to Level 5 (*optimize*) and address recommendations cited in the draft report. Furthermore, we recognize that the draft report states the following and the Bureau offers responses to these statements:

The Bureau is operating at a Level-4 maturity for the **Identify** function.

- The Bureau's Risk Management program is operating at Level-4 maturity (*Managed and Measurable).* The Bureau ensures that its information systems are subject to the monitoring processes defined within its Information Security Continuous Monitoring (ISCM) program. In addition, the Bureau maintains qualitative and quantitative performance measures related to its plans of action and milestones process. In FY2021, the Bureau will continue to improve its enterprise and cybersecurity risk management programs by defining the risk appetite statement, risk tolerance levels, and work to implement processes that will prohibit future instances of systems being placed into production without completion of Security Assessment & Authorization (SA&A) activities.

The Bureau is operating at a Level-3 maturity for the **Protect** function.

- The Bureau's Configuration Management program is operating at level-3 maturity (*Consistently Implemented*). The Bureau employs network access controls to detect unauthorized hardware. Furthermore, it tracks and reports on performance measures related to its change control activities. In addition, this year the Bureau centralized multiple configuration management processes, for hardware and software inventory and change requests, into a single tool. The agency's configuration management database has also been integrated into this tool, enabling the agency to better track changes back to the approved request. The Bureau will continue updating separation of duties policies and

configurations in the change request tool to restrict the ability of users to close change requests outside the approved group. Lastly, the Bureau will continue migrating all Bureau issued mobile phones to a new mobile device management system, which will provide the ability to enforce current patches on the mobile phones.

- The Bureau's Identity and Access Management (ICAM) program is operating at Level-3 maturity (Consistently Implemented). The Bureau has performed duties indicative of a higher maturity level for this domain, such as allocating resources to effectively implement ICAM activities and holding personnel accountable for carrying out their roles and responsibilities. In addition, the Bureau has developed an ICAM roadmap, which defines an implementation strategy for identity and access management objectives related to provisioning multifactor authentication and zero trust architecture by FY2022. In FY2021, the Bureau plans to improve its identity and access management program by implementing tools that will enforce multifactor authentication (MFA) for privileged and non-privileged users. In addition, a new configuration management tool will be used to provide better maintenance of user-access agreements and rules-of-behavior forms for individuals with privileged access.

- The Bureau's Data Protection and Privacy program is operating at Level-4 maturity (*Managed and Measurable).* The Bureau has defined, communicated, and implemented its tailored privacy awareness and role-based training program. The Bureau has also consistently implemented its policies and procedures regarding the encryption of information at various states and restricts the use of removable storage devices. The Bureau has also implemented encryption for sensitive data at-rest and in-transit, as appropriate, and the Bureau restricts the use of removable storage devices. In FY2021, the Bureau will continue improving its data protection and privacy program by consistently deploying exfiltration tools across the enterprise to monitor and block access to known Internet storage sites and prevent exfiltration of data to unauthorized sites and systems.

- The Bureau's Security Training program is operating at Level-4 maturity (*Managed and Measurable).* This year, the Bureau has completed a knowledge, skills, and abilities (KSAs) assessment of its employees. In addition, the Bureau has updated its phishing program to reflect COVID-19 considerations and is also providing tips regarding security considerations specific to the pandemic to its workforce. In FY2021, the Bureau plans to improve its security training program by updating its policies and procedures in a timelier manner. Additionally, the Bureau will implement targeted phishing exercises and obtain metrics on the effectiveness of its security training offerings in relation to closing gaps in the National Initiative for Cybersecurity Education (NICE) framework.

The Bureau is operating at a level-4 maturity for the **Detect** function.

- The Bureau's ISCM program continues to operate at Level-4 maturity *(Managed and Measurable).* The Bureau has defined and communicated roles and responsibilities for ISCM stakeholders, along with identifying skill gaps and training needs for ISCM staff. In

addition, the Bureau has integrated metrics on the effectiveness of its ISCM program across the organization. In FY2021, the Bureau will improve its ISCM program by providing a defined risk-appetite statement and associated risk-tolerance levels and integrating the program with the Enterprise Risk Management (ERM) processes.

The Bureau is operating at a Level-4 maturity for the **Respond** function.

- The Bureau's Incident Response program continues to operate at Level-4 maturity (*Managed and Measurable).* The Bureau has implemented a new incident ticketing system that provides closer integration with configuration management activities. In addition, the agency continues to capture and assess incident response performance measures. Further, our analysis showed that the Bureau intakes and analyzes alerts, advisories, and indicators of compromise from the Department of Homeland Security (DHS). The improvement in the categorization of incident tickets, resulted in the closing of a 2019 recommendation. Additionally, the Bureau is tracking additional metrics related to the effectiveness of incident response processes and has created plans to further mature capabilities in this area. In FY2021, the Bureau will improve its incident response program by utilizing automated features in the new incident ticketing system to continue remediating the backlog of security tickets that have not gone through peer review.

The Bureau is operating at a Level-3 maturity for its **Recover** function.

- The Bureau's Contingency Planning program is operating at a Level-3 maturity (*Consistently Implemented).* The Bureau has documented its roles and responsibilities for contingency in the Bureau's Continuity of Operations Plan. Additionally, the Bureau continues to implement backup and storage processes in accordance with CFPB policies and procedures. In FY2021, the Bureau will improve the contingency planning program by prioritizing the development of system-level Business Impact Analysis (BIAs), as appropriate, and incorporate the results into contingency planning strategies and processes.

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

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

Sincerely,

Donna Roy
Chief Operating Officer and Acting Chief Information Officer

Response to recommendations presented in the Draft OIG Report, "*2020 Audit of the Bureau's Information Security Program*."

<u>Recommendation 1:</u> Ensure that (a) change control policies and procedures address separation of duties in the change management lifecycle, and (b) separation of duties is enforced in the Bureau's change control tool.

<u>Management Response:</u>

Management concurs with the recommendation. The Enterprise Architecture team responsible for change management has submitted and has received approvals for an enhancement to the change management workflow on the ServiceNow platform that is designed to restrict who may close a change management record. This is designed to permit the appropriate levels of change request process steps, information inclusion, notifications and approvals to take place prior to the completion of the change request process. As a result of this enhancement, and in line with separation of duties, only a member of the Change Management team may record Technical Change Advisory Board (TCAB) approvals and close the change request after all applicable steps, reviews and information are included.

Abbreviations

BIA	business impact analysis
CIO	chief information officer
DHS	U.S. Department of Homeland Security
DLP	data loss protection
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
HVA	high-value asset
ICAM	identity, credential, and access management
ICT	information and communications technology
IG	inspector general
ISCM	information security continuous monitoring
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	personally identifiable information
SA&A	security assessment and authorization
SP 800-34	Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
SP 800-53	Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
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 (ISCM) for Federal Information Systems and Organizations*
TIC	Trusted Internet Connections
US-CERT	United States Computer Emergency Readiness Team

Report Contributors

Khalid Hasan, Senior OIG Manager for Information Technology
Andrew Gibson, OIG Manager
Jeff Woodward, Senior IT Auditor
Martin Bardak, IT Auditor
Justin Byun, IT Auditor
Trang Do, IT Auditor
Kaneisha Johnson, IT Auditor
Fay Tang, Statistician
Alexander Karst, Senior Information Systems Analyst
Hau Clayton, Senior Forensic Auditor
Monica Cook, Forensic Auditor
Victor Calderon, OIG Manager
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