

Bureau of Consumer Financial Protection

2019 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, 2019-IT-C-015, October 31, 2019

2019 Audit of the Bureau's Information Security Program

Findings

Since our review last year, the Bureau of Consumer Financial Protection (Bureau) has matured its information security program. Specifically, we found that the Bureau's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. For instance, the Bureau's information security continuous monitoring process is effective, with the agency enhancing the functionality of its security information and event-monitoring tool. Further, the Bureau's incident response process is similarly effective, with the agency using multiple tools to detect and analyze incidents and track performance metrics.

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 Cybersecurity Framework security functions—*identify, protect, detect, respond, and recover*—to ensure that its program remains 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. Further, the Bureau has not identified its high-value assets and determined what governance and security program changes may be needed to effectively manage security for those assets. Additionally, we identified improvements needed in the implementation of the Bureau's security assessment and authorization processes to manage security risks prior to deploying Bureau systems. We also identified improvements needed in database security, timely remediation of vulnerabilities, and patching of mobile phone operating systems.

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 data protection and privacy, incident response, and contingency planning. We are leaving open 7 recommendations in the areas of risk management, configuration management, and identity and access management. We will continue to monitor the Bureau's progress in these areas as part of future FISMA reviews.

Recommendations

This report includes 7 new recommendations designed to strengthen the Bureau's information security program in the areas of risk management, identity and access management, data protection and privacy, incident response, and contingency planning. In its response to a draft of our report, the Bureau 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 agencies' information security programs across several areas. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.



Office of Inspector General

Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Recommendations, 2019-IT-C-015, October 31, 2019

2019 Audit of the Bureau's Information Security Program

| Number | Recommendation | Responsible office |
|--------|---|--|
| 1 | Determine which components of an HVA program are applicable to the Bureau and ensure the implementation of a governance structure and HVA-specific baselines and planning activities, as appropriate. | Office of the Chief Operating Officer, Office of the Chief Data Officer, and Office of Technology and Innovation |
| 2 | Ensure that established SA&A processes are performed prior to the deployment of all cloud systems used by the Bureau. | Office of Technology and Innovation |
| 3 | Ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonprivileged users. | Office of Technology and Innovation |
| 4 | Conduct a comprehensive, risk-based review to determine the optimal resources and process for prioritizing the review and adjudication of background investigations. | Office of Administrative Operations |
| 5 | Perform a risk assessment to determine <ol style="list-style-type: none">the optimal deployment of the Bureau's technology for monitoring and controlling data exfiltration to all network access points.appropriate access to internet storage sites. | Office of Technology and Innovation |
| 6 | Ensure that data captured in security and privacy incident processes and tickets are accurate, consistent, and of high quality. | Office of Technology and Innovation and Office of the Chief Data Officer |
| 7 | Ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes. | 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, 2019

TO: Distribution List

FROM: Peter Sheridan 
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2019-IT-C-015: *2019 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 their agency's information security program and practices. As part of our work, we analyzed key FISMA-related data and conducted technical testing; the detailed results of that testing 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 2019 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 recommendations and outline actions that have been or will be taken to address our recommendations. 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: Tiina Rodrigue
Tannaz Haddadi
Marianne Roth
Kirsten Sutton
Elizabeth Reilly
Dana James
Lauren Hassouni
Carlos Villa

Distribution:

Katherine Sickbert, Acting Chief Information Officer
Kate Fulton, Chief Operating Officer

Martin Michalosky, Chief Administrative Officer
Ren Essene, Chief Data Officer



Contents

| | |
|--|-----------|
| Introduction | 7 |
| Objectives | 7 |
| Background | 7 |
| FISMA Maturity Model | 9 |
| Analysis of the Bureau’s Progress in Implementing Key FISMA Information Security Program Requirements | 11 |
| Identify | 12 |
| Risk Management | 12 |
| Protect | 19 |
| Configuration Management | 20 |
| Identity and Access Management | 24 |
| Data Protection and Privacy | 27 |
| Security Training | 31 |
| Detect | 32 |
| Information Security Continuous Monitoring | 32 |
| Respond | 34 |
| Incident Response | 34 |
| Recover | 37 |
| Contingency Planning | 37 |
| Status of Prior Years’ Recommendations | 40 |
| Appendix A: Scope and Methodology | 43 |
| Appendix B: Management Response | 44 |
| Abbreviations | 49 |



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 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 2019 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.3, April 9, 2019.

³ 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, 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

As noted in DHS’s IG FISMA reporting metrics, one of the goals of the annual IG FISMA evaluation is to assess agencies’ progress toward achieving outcomes that strengthen federal cybersecurity, including implementation of the administration’s priorities. Two of these priorities are agency progress in implementing high-value asset (HVA) programs and supply chain management security best practices. Specifically, Office of Management and Budget (OMB) Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, requires all federal agencies to establish an HVA governance structure and take a strategic, enterprisewide view of cyber risks to HVAs.⁴ Additionally, the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2018 (SECURE Technology Act) was passed to, in part, strengthen federal acquisition supply chain security.⁵ As such, the IG FISMA reporting metrics have been updated to gauge the effectiveness of an agency’s HVA program as well as its preparedness for addressing the SECURE Technology Act, while recognizing that specific guidance on supply chain risk management will be issued later.

⁴ OMB Memorandum M-19-03 notes that agencies may designate federal information or information systems as HVAs when (1) the information or information system that processes or stores the information is of high value, (2) the agency that owns the HVA cannot accomplish its primary mission-essential function within expected time frames without the information or information system, or (3) the information or information system serves a critical function in maintaining the security and resilience of the federal enterprise.

⁵ Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Pub. L. No. 115-390, 128 Stat. 3073 (2018) (codified at 44 U.S.C. §§ 3553–3554).

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 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.

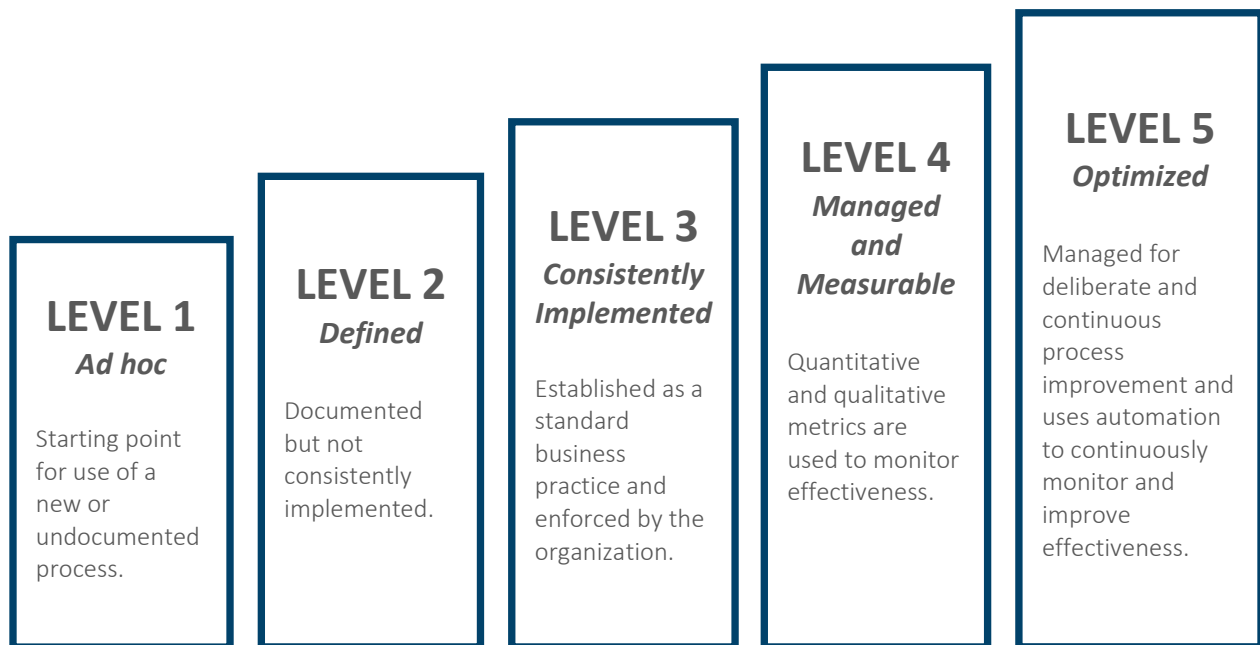
The five levels of the IG FISMA maturity model are

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 the 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 a maturity model. Details on the scoring methodology for the maturity model can be found in appendix A.

⁶ 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.

Figure 1. FISMA Maturity Model Rating Scale



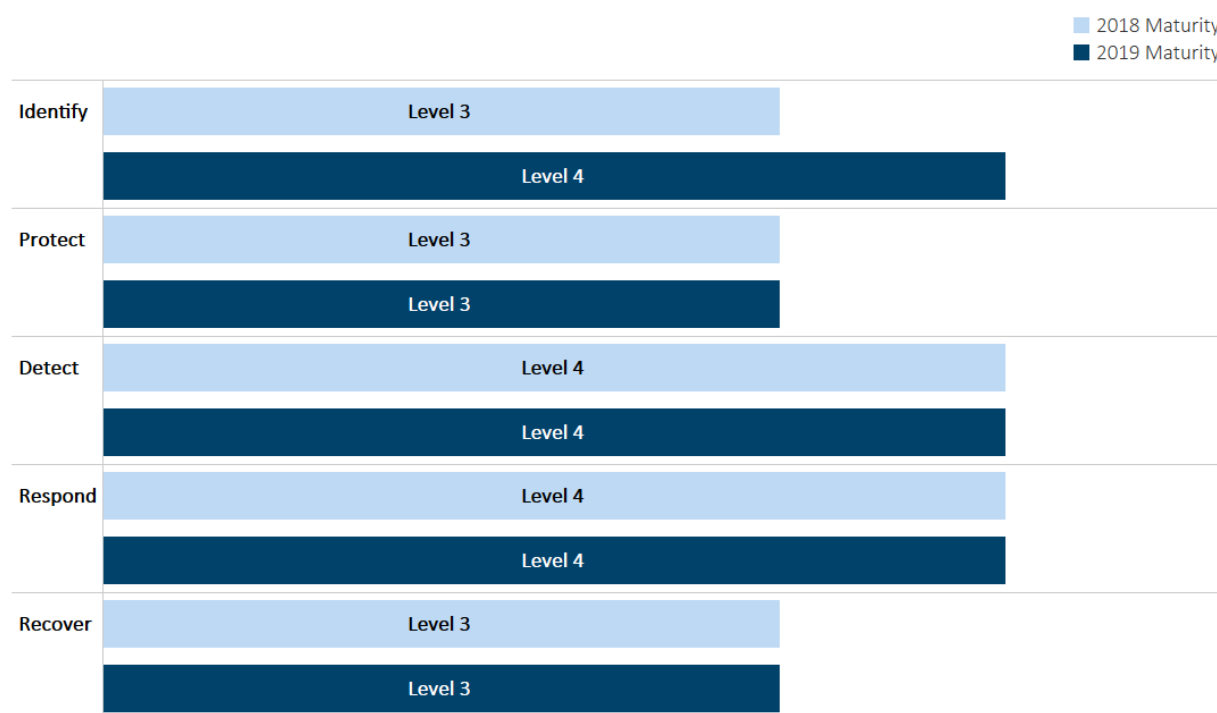
Source. OIG analysis of DHS IG FISMA reporting metrics.



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 hardware asset management program by employing automation to track the life cycle of its hardware assets. Although the agency has strengthened its information security program since our 2018 FISMA review, it has further opportunities to ensure that the program is effective across specific FISMA domains in all five NIST Cybersecurity Framework security functions: *identify*, *protect*, *detect*, *respond*, and *recover*. Our report includes 7 recommendations in these areas as well as several items for management's consideration.

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



Source. OIG analysis.

⁷ To determine the maturity of the Bureau's information security program, we used the scoring methodology outlined in the IG FISMA reporting metrics. Appendix A provides additional details on the scoring methodology.

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. Examples of the areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Bureau's processes for enterprise risk management (ERM), securing HVAs, developing and implementing an enterprise architecture, asset management, and using plans of action and milestones to manage the remediation of security weaknesses.

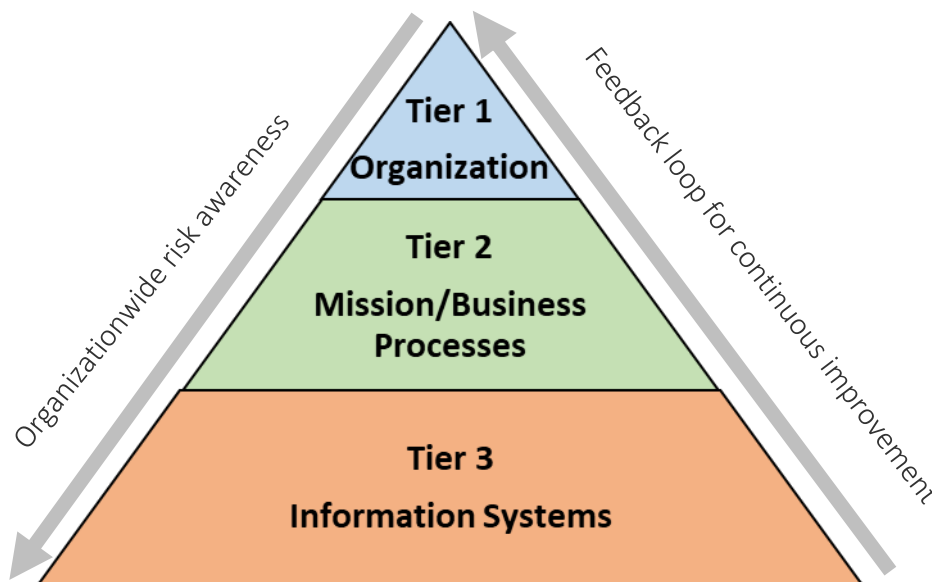
Risk Management

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. Risk management is further emphasized in OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which states that an effective ERM program promotes a common understanding for recognizing and describing potential risks that can affect an agency's mission. Such risks can include cybersecurity,⁸ strategic, market, legal, and reputational.

The relationships between cybersecurity risk management and ERM are further outlined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (SP 800-39), which notes that effective risk management involves integration of activities at the enterprise, mission and business process, and information system levels. As depicted in figure 3, the risk management process is to 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 all stakeholders having a shared interest in the success of the organization.

⁸ According to Executive Order, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, cybersecurity risk management refers to the full range of activities undertaken to protect information technology and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents.

Figure 3. The Three Tiers of Risk Management



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

Tier 1 addresses risk from an organizational perspective, providing the context for risk management activities carried out by the organization at tiers 2 and 3. NIST SP 800-39 notes that at tier 1, organizations are required to frame risk, which involves establishing the overall context for risk-based decisions. This context is established through the development of an ERM program. ERM refers to an effective agencywide approach to addressing the full spectrum of the agency's external and internal risks and includes the establishment of an organizationwide risk management strategy. Examples of ERM activities include the establishment of an enterprisewide risk management strategy and a supporting governance structure that includes the designation of a risk executive function. Additionally, ERM activities include the definition of the organization's risk appetite, risk tolerance, and risk profile.⁹

NIST SP 800-39 also notes that a key output of tier 1 risk management activities is the prioritization of mission and business functions. Specifically, more-critical mission and business functions necessitate a greater degree of risk management investments than those functions that are deemed less critical. NIST SP 800-39 further states that the determination of the relative importance of the mission and business functions, and hence the level of risk management investment, is decided at tier 1, executed at tier 2, and influences risk management activities at tier 3.

Tier 2 addresses risk from the mission and business process perspective and is informed by the risk context, decisions, and activities at tier 1. Risk management activities at tier 2 include prioritizing mission and business processes and defining the types and criticality of information needed to successfully execute the mission and business processes. These activities, along with the prioritization of mission and

⁹ 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.

business functions at tier 1, can serve as a key input into the development of an HVA program. OMB Memorandum M-19-03 requires agencies to take a strategic, enterprisewide view of cyber risk and bolster protections of their HVAs to improve risk management across the government.¹⁰ HVAs are information and information systems that are deemed the most critical and high impact to agency and federal government operations.

Another key tier 2 activity, as noted in SP 800-39, is the incorporation of information security requirements into mission and business processes, resulting in the development of an enterprise architecture. An enterprise architecture provides a disciplined and structured approach to achieving consolidation, standardization, and optimization of information technology (IT) assets that are employed within organizations. The information security architecture, which is a component of the enterprise architecture, influences and guides the allocation of information protections needs, which affects the allocation of specific security controls at tier 3.

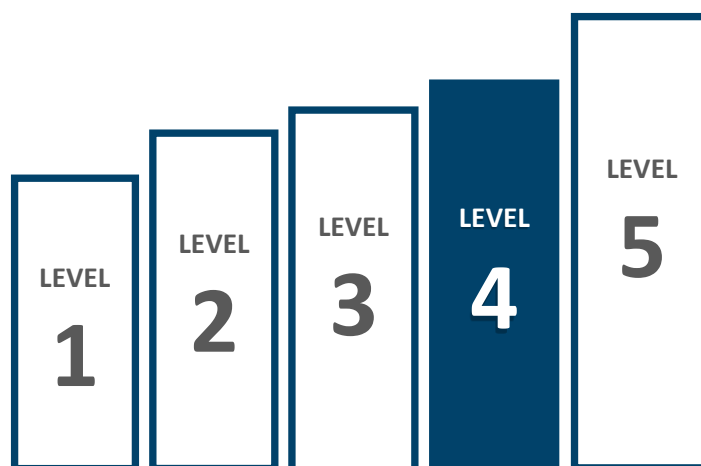
Tier 3 addresses risk from an information system perspective and is guided by the risk context, risk decisions, and risk activities at tiers 1 and 2. Tier 3 risk management activities include the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls for all of the organization's information systems. NIST SP 800-39 notes that the risk management activities at tier 3 reflect the organization's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual information systems supporting the mission and business functions of organizations. Such requirements include specific control considerations for an organization's HVAs.

Current Security Posture

We found that the Bureau has matured its risk management program from a level-3 maturity in 2018 to a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 4). For instance, 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 plans of action and milestones process.

We have made several recommendations in prior FISMA reports for strengthening the Bureau's risk management program, including in the areas of insider threat and ERM. Our 2016 FISMA audit report included a recommendation for the CIO to

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



Source. OIG analysis.

¹⁰ In November 2017, DHS published the *High Value Asset Control Overlay* to provide technical guidance to federal civilian agencies on securing HVAs.

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.¹¹ This year, the Bureau developed an *Insider Threat Program Communications Plan* that defines various components of an insider threat program, including communication channels and roles and responsibilities. However, we found that the Bureau has not fully implemented its data loss prevention tool across the enterprise. As such, we are leaving our 2016 recommendation open and will continue to monitor the Bureau's efforts in this area as part of our future FISMA reviews.

In addition, 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.¹² This year, we found that the Bureau has updated its risk profile and conducted an agencywide security and privacy risk assessment. However, the Bureau has not approved a risk appetite statement and finalized tolerance levels. As such, we are leaving this recommendation open and will continue to monitor the Bureau's efforts in this area as part of our future FISMA reviews.

Opportunities for Improvement

We identified several opportunities to strengthen the agency's risk management program at the organization level (tier 1), mission and business process level (tier 2), and information system level (tier 3). We believe that strengthening these areas will allow the Bureau to improve its risk management program.

Organization Level (Tier 1)

One key output of tier 1 is the development of an ERM program to address the full spectrum of the agency's risks and provide the overall context in which risk management decisions are made across the organization. As noted above, the Bureau is still working to define its risk appetite statement and tolerance levels as part of its ERM implementation. Completion of the risk appetite statement and tolerance levels will affect risk-based decisionmaking at other tiers. Further, we noted that the Office of Technology and Innovation is using an automated tool to track system-level risk management activities. However, from an organizationwide perspective, the Bureau has not determined 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. As mentioned in our 2017 and 2018 FISMA reports, we realize that the implementation of such technologies depends on the Bureau fully implementing its ERM management strategy and related components. Further, such tools are offered through DHS's Continuous Diagnostics and Mitigation (CDM) program. As further detailed in the information security continuous monitoring (ISCM) section of our report, the Bureau is working with DHS to determine which components of the CDM program it will implement. As part of this effort, we believe that the Bureau should determine whether there are tools offered through CDM that will meet the agency's needs in this area. Because the Bureau's CDM implementation is in progress, we are not making a recommendation in

¹¹ Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*, [OIG Report 2016-IT-C-012](#), November 10, 2016.

¹² Office of Inspector General, *2017 Audit of the CFPB's Information Security Program*, [OIG Report 2017-IT-C-019](#), October 31, 2017.

this area. We will continue to monitor the Bureau's efforts to use technology to strengthen its ERM program.

Mission and Business Process Level (Tier 2)

As noted earlier, a key activity in tier 2 is developing and implementing an HVA program for the information and information systems that are deemed the most critical and high impact to agency and federal government operations. Specifically, OMB Memorandum 19-03 requires agencies to take a number of steps to protect their HVAs against evolving cyber threats. These steps are outlined in table 2 and collectively represent the components of an HVA program.

Table 2. Key HVA Program Requirements

| Requirement | Description |
|--------------------------------------|--|
| Establish enterprise HVA governance | Designate an HVA governance structure to incorporate HVA activities into broader agency activities, such as ERM, contracting processes, and contingency planning. |
| Improve the designation of HVAs | Identify and designate federal information or a federal information system as an HVA based on information value, support of mission-essential functions, and support of a critical function in maintaining the security and resilience of the federal civilian enterprise. |
| Implement data-driven prioritization | Allocate appropriate resources and ensure the effective protection of HVAs through collaboration and data-driven prioritization. |
| Increase the trustworthiness of HVAs | Implement systems security engineering principles for all HVAs to include security and privacy requirements. |
| Protect the privacy of HVAs | Ensure that privacy documentation and materials are maintained for HVAs that create, process, use, store, maintain, disseminate, disclose, or dispose of personally identifiable information. |

Source. OIG analysis of OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018.

The Bureau has not established a formal HVA program and properly identified its HVAs, in accordance with federal guidance. Specifically, the Bureau initially classified all of its information systems as HVAs. We did not find evidence, however, that the Bureau arrived at this determination by using DHS and OMB guidance or by performing a formal assessment to identify its HVAs. Office of Technology and Innovation officials stated that they are in the process of performing a comprehensive assessment to determine the agency's HVAs and anticipate completing this effort by the end of the third quarter of 2019. We believe that by properly identifying its HVAs and establishing an overall HVA program, as appropriate, the Bureau will have greater assurance that its key systems and data are adequately protected.

Information Systems Level (Tier 3)

A key step in tier 3 is the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls for all of the organization's information systems, including HVAs. With respect to HVAs, OMB Memorandum M-19-03 requires that agencies implement the system security engineering principles outlined in NIST Special Publication 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, and ensure that security and privacy requirements for all HVAs reflect these principles. In addition, DHS has issued guidance that provides additional specifications for protections applied to HVAs.¹³ This guidance notes that the additional HVA control specifications are intended to be applied after an agency has selected and applied either the high or moderate security baselines for all information systems specified by NIST. We found that while the Bureau has developed control baselines for its information systems in accordance with NIST guidance, the agency has not defined additional security controls and enhancements that will apply to its HVAs. We believe that as the Bureau defines its HVA program, it should ensure that any additional security controls and enhancements beyond those that apply to all Bureau systems are identified, defined, and communicated.

Further, we identified improvements needed in the implementation of the Bureau's security assessment and authorization (SA&A) process. Specifically, we found that the agency deployed two of three cloud-based systems that we sampled without completing a comprehensive system security plan, conducting an agency-specific risk and security controls assessment, or granting an authorization to operate (ATO). Bureau officials attributed this issue to an overreliance on vendors and internal oversight. Further, once we notified the Bureau of these issues, agency officials took immediate steps to ensure that SA&A activities were initiated. As a result of these weaknesses, there is increased risk that cloud-based systems in use do not meet the Bureau's information security requirements. For example, as noted in the identity and access management section of our report, we found weaknesses in the Bureau's management of user-access forms for one of the cloud-based systems that had not gone through the agency's SA&A process. We believe that this issue may have been flagged if the Bureau's SA&A process had been followed prior to system deployment.

The Bureau's *Information Security Program Policy* notes that the agency uses the foundational process of SA&A to document and manage the security posture of new and existing systems, including cloud systems, and their operating environments. Table 3 outlines key components of the Bureau's SA&A processes as they relate to system security planning, risk and security controls assessment, and ATO.

¹³ U.S. Department of Homeland Security, *High Value Asset Control Overlay*, Version 1.0, November 2017.

Table 3. Key Activities Supporting the Bureau’s SA&A Process

| Activity | Requirement and description |
|--------------------------------------|--|
| System security planning | The system security plan specifies the security requirements applicable to the system and the protection mechanisms implemented to meet those requirements. System owners are required to develop a system security plan for each major information system. |
| Risk and security control assessment | The Bureau has developed a formalized process to assess the risks associated with the operation of agency information systems. As part of this process, a security controls assessment is required to determine whether selected security controls are implemented correctly, operate as intended, and are effective in achieving security objectives. The mitigation of weaknesses that are discovered through this process is managed through a plan of action and milestones. |
| ATO | An ATO is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations. All new Bureau systems, including cloud systems, are required to be granted an ATO prior to being operated in a production environment. |

Source. OIG analysis of the Bureau’s information security program and risk management process.

In our 2019 report, *The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP*, we identified a similar issue with respect to a cloud system approved by the Federal Risk and Authorization Management Program (FedRAMP) and used by the Bureau.¹⁴ Specifically, we found that the Bureau did not ensure that its SA&A process was followed for a FedRAMP-approved cloud system used by the agency to support its call center operations prior to its deployment.¹⁵ We recommended that the CIO ensure that established SA&A processes are (1) performed prior to the deployment of all FedRAMP-approved cloud systems used by the Bureau and (2) used to make an agency-specific authorization decision for the system that is in production and noted in our report. The issues we identified in the current report are for Bureau-used cloud systems that are *not* provided through FedRAMP, and, as such, we are making a recommendation for the Bureau to strengthen its SA&A processes for all cloud systems. We believe that by ensuring that SA&A activities are completed prior to onboarding cloud systems, the Bureau will have greater assurance that controls are effectively implemented to protect sensitive agency information.

¹⁴ FedRAMP was established in December 2011. One of the goals of FedRAMP is to provide a cost-effective, risk-based approach to the adoption and use of cloud service by federal agencies. The Bureau uses several FedRAMP-approved cloud systems.

¹⁵ Office of Inspector General, *The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP*, [OIG Report 2019-IT-C-009](#), July 17, 2019.

Recommendations

We recommend that the Chief Operating Officer, the Chief Data Officer, and the CIO

1. Determine which components of an HVA program are applicable to the Bureau and ensure the implementation of a governance structure and HVA-specific baselines and planning activities, as appropriate.

We recommend that the CIO

2. Ensure that established SA&A processes are performed prior to the deployment of all cloud systems used by the Bureau.

Management Response

The Acting CIO concurs with these recommendations. The Acting CIO notes that the Bureau will review how an HVA program may apply to the agency to ensure that resulting governance processes incorporate related activities, such as identification of HVA and applicable controls or processes, into ERM. Further, the Acting CIO notes that, moving forward, all Bureau systems will undergo the SA&A processes before being deployed for production use.

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.

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. Table 4 summarizes the security domains that are included in this security function and the associated assessment areas, as outlined in the IG FISMA reporting metrics, that we assessed.

Table 4. *Protect* Function Security Domains and Selected Components

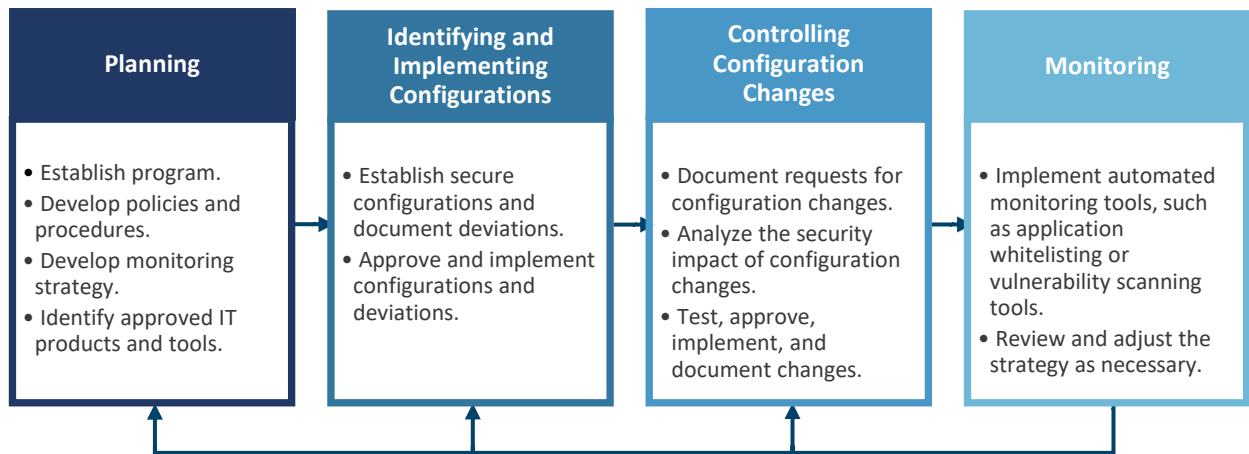
| Security domains | Examples of components assessed by IGs |
|--------------------------------|---|
| Configuration management | Configuration management plans, configuration settings, flaw remediation, and change control |
| Identity and access management | Identity credential and access management 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

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*, 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 5).

Figure 5. Security-Focused Configuration Management Phases



Source. NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*.

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.

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), notes that organizations should install security-relevant software and firmware updates within organization-defined time frames and incorporate flaw remediation into configuration management processes. 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 and can restrict access if the device's operating system is not up to date.

Current Security Posture

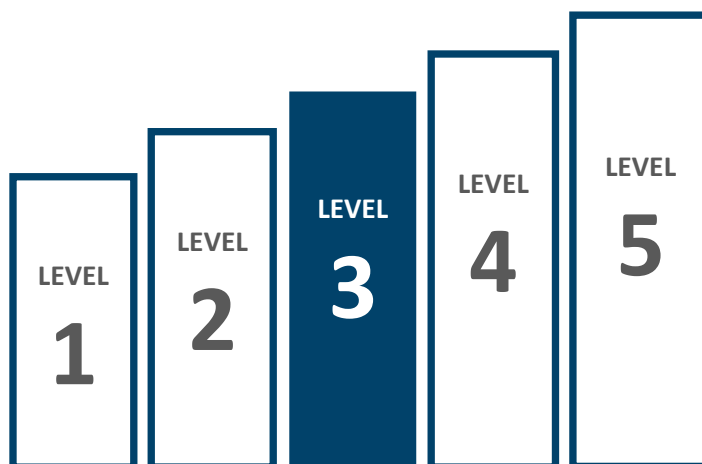
The Bureau's configuration management program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level (figure 6). For instance, the Bureau employs network access controls to detect unauthorized hardware. Further, the Bureau tracks and reports on performance measures related to its change control activities.

Opportunities for Improvement

Our previously identified issues in the areas of secure database configurations, vulnerability remediation, and mobile phone patch management continue to represent opportunities for the Bureau to mature its configuration management program. Specifically, our vulnerability scanning continues to identify weaknesses in the Bureau's database-level security configurations.¹⁶ Similar to last year, the weaknesses identified relate to unsecure database configurations, including for controls related to audit and accountability, and system and information integrity. We initially included a recommendation to strengthen database- and application-level configuration management processes in our 2014 FISMA report.

Specifically, 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.¹⁷ Last year, we found that the Bureau has implemented an application-level vulnerability-scanning tool, which the agency is using for its web applications.¹⁸ This year, we found that the Bureau is still in the processes of identifying and implementing a database-level vulnerability scanning product. We believe that the lack of a database-level vulnerability scanning process is a key contributing cause for the database configuration weaknesses we continue to identify. Although we are not making additional recommendations in this area, we strongly suggest that the Bureau continue to prioritize the implementation of an automated solution and process to periodically assess and manage database-level security configurations. We are leaving our

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



Source. OIG analysis.

¹⁶ The Bureau provided us with authorized access to its network and administrative credentials to perform scanning within its internal network. The detailed results of our follow-up work in this area will be transmitted to the Bureau under a separate, restricted cover due to the sensitive nature of the information.

¹⁷ Office of Inspector General, *2014 Audit of the CFPB's Information Security Program*, [OIG Report 2014-IT-C-020](#), November 14, 2014.

¹⁸ Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, [OIG Report 2018-IT-C-018](#), October 31, 2018.

2014 recommendation open and will continue to follow up on the Bureau's efforts in this area as a part of future FISMA reviews.

In addition, our 2018 FISMA report includes a recommendation for the CIO to strengthen configuration management processes by (1) remediating configuration-related vulnerabilities in a timely manner and (2) ensuring that optimal resources are allocated to perform vulnerability remediation activities.¹⁹ We continue to find that the Bureau is not timely remediating numerous critical or high-risk vulnerabilities in agency systems that it has identified through its own vulnerability scanning.²⁰ Further, our operating system-level vulnerability scanning identified a number of critical or high-risk vulnerabilities that had previously been identified by the Bureau's internal vulnerability scans several months earlier.²¹ The Bureau's *Information Security Standards* (CS-S-01) requires that critical, high, moderate, and low vulnerabilities be remediated timely, and that for critical vulnerabilities, remediation be performed within 30 days. Bureau officials continue to note that the key cause for the delays in mitigating technical vulnerabilities is a lack of resources.

While the Bureau took steps to strengthen security controls in this area during our review, we believe that an overall process to ensure timely remediation of security vulnerabilities could better protect Bureau systems and data from compromise. As such, we are leaving our 2018 recommendation open and will monitor the Bureau's efforts in this area as part of our future FISMA reviews.

Finally, our 2018 FISMA report includes a recommendation for the CIO to develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.²² We continue to identify Bureau mobile devices that do not have current operating system patches applied. Bureau officials stated that by the end of 2019, the agency would update its policy to require that agency-issued mobile phones have the latest operating system and deploy a new tool to enforce the application of current patches for mobile phone operating systems. As such, 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.

¹⁹ Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, [OIG Report 2018-IT-C-018](#), October 31, 2018.

²⁰ While the Bureau has not implemented a database-level vulnerability scanning process or tool, the agency regularly performs vulnerability scans of its network and operating systems.

²¹ The Bureau provided us with special authorized access to the network and administrative credentials to perform operating system-level scanning within its internal network.

²² Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, [OIG Report 2018-IT-C-018](#), October 31, 2018.

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).

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 management 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.

Figure 7. ICAM Conceptual Design

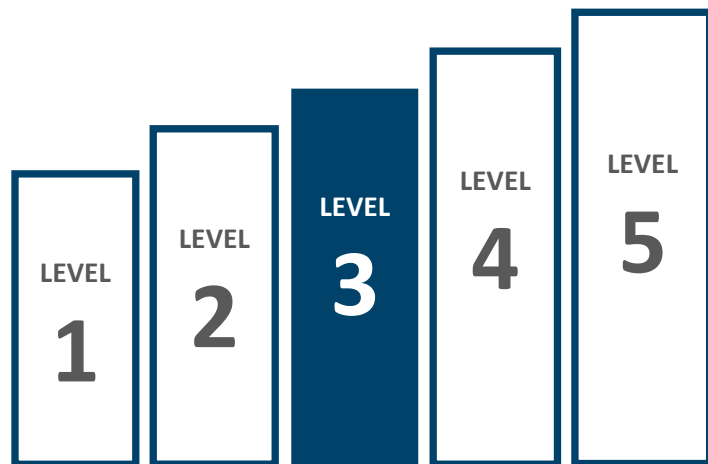


Source. CIO Council, *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance*.

Current Security Posture

The Bureau's identity and access management program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing certain activities indicative of a higher maturity level (figure 8). For instance, the Bureau is allocating resources to effectively implement ICAM activities and holding personnel accountable for carrying out their roles and responsibilities. The Bureau continues to consolidate ICAM investments across the agency and has defined an implementation strategy. Additionally, the Bureau has strengthened identity and access controls for its remote access program. Specifically, the Bureau is using enhanced features offered by its security information, event-monitoring, and antivirus software to perform more detailed user activity reviews for remote access sessions.

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



Source. OIG analysis.

Opportunities for Improvement

Our previously identified issues in the areas of maintaining user-access agreements and rules-of-behavior forms for individuals with privileged access and requiring the use of multifactor authentication sign-on for Bureau users continue to represent opportunities for the Bureau to mature its identity and access management program. This year, we also identified improvements needed in the maintenance of user-access forms for general users and in the timely adjudication of background investigations.

In our 2018 FISMA audit report, we found that the Bureau was not consistently managing and updating its user-access agreement and rules-of-behavior documentation for a sample of privileged or administrative users. We recommended 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.²³ This year, we sampled user-access agreement and rules-of-behavior documentation for a total of 17 privileged users for the three Bureau cloud systems we sampled.²⁴ We found that for 14 of these privileged users, user agreement forms did not include appropriate approval of the need for access, and rules-of-behavior documents were not on file. As such, we are keeping our 2018 recommendation open and will continue to monitor the Bureau's efforts in this area as part of future FISMA reviews.

²³ Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, [OIG Report 2018-IT-C-018](#), October 31, 2018.

²⁴ Per the Bureau's cybersecurity policy, a privileged user is defined as an individual who has been granted elevated privileges, which are typically allocated to system administrators, network administrators, and others who are responsible for system or application control, monitoring, or administration functions.

Further, we sampled 20 nonprivileged users for a select Bureau cloud system and found that user-access agreements were not completed for any of the users. For these users, rules-of-behavior forms were completed instead; however, these forms do not contain supervisory approval of the need for access. The Bureau's access controls policies require nonprivileged users to have authorized access to the information system based on valid access authorization and intended system usage. Further, as referenced in the risk management section of this report, this issue occurred for the same cloud system that had not gone through the Bureau's SA&A process prior to being implemented in a production environment. We believe that completion of user-access agreements prior to provisioning access to systems will provide the Bureau with greater assurance that only individuals with a business need have access to agency systems. Our report includes a new recommendation in this area.

Additionally, as we have previously reported, the Bureau has not fully implemented multifactor authentication for logical access to its information systems. In our 2017 FISMA audit report, we found that the Bureau had 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.²⁵ 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 Bureau implemented several technical solutions that in totality did not fully meet federal requirements for multifactor authentication. Specifically, DHS guidance requires users to authenticate to an agency's network using a two-factor PIV credential or other Identity Assurance Level 3/Authenticator Assurance Level 3 credential. NIST Special Publication 800-63, *Digital Identity Guidelines*, notes that in order to authenticate at Authenticator Assurance Level 3, possession and control of two distinct factors are required. The technical solutions implemented by the Bureau did not meet these requirements. Bureau officials explained that, as they continue to move toward a cloud-only infrastructure, they plan to incorporate a hybrid approach to ICAM and are evaluating various initiatives for multifactor authentication in such an environment. As such, we are leaving our 2017 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.

Finally, we found that the Bureau is not reviewing and adjudicating background investigation results received from the Office of Personnel Management (OPM) in a timely manner. Specifically, we identified 3 of a sample of 37 Bureau employees and contractors who had completed background investigations by OPM but had not received a review and adjudication by the Bureau in approximately 5 months. This included Bureau personnel with elevated access to systems with sensitive data.²⁶ Further, Bureau officials informed us that overall they have a backlog of approximately 300 background investigations completed by OPM for which they need to perform adjudication. Approximately 35 percent of these are for new

²⁵ Office of Inspector General, *2017 Audit of the CFPB's Information Security Program*, [OIG Report 2017-IT-C-019](#), October 31, 2017.

²⁶ In accordance with the Bureau's personnel security policy, employees and contractors are provided access to agency systems after the completion of a fingerprint check.

employees or contractors, while the remaining 65 percent are for re-investigations of current employees and contractors.²⁷

The Bureau's *Personnel Security Policy* requires that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened. The adjudication and final clearance determinations are the final stage of the process to determine whether an individual is deemed eligible for access. The Bureau cited resource constraints as a contributing factor for not adjudicating completed background investigations in a timely manner. We believe that the recent lifting of the agency's hiring freeze may also affect the timely adjudication of background investigations moving forward. We believe that timely adjudication of the completed background investigations from OPM could yield additional information necessary to determine a person's eligibility to access Bureau systems. Further, timely adjudication of background investigations could help mitigate risks from insider threats.

Recommendations

We recommend that the CIO

3. Ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonprivileged users.

We recommend that the Chief Administrative Officer

4. Conduct a comprehensive, risk-based review to determine the optimal resources and process for prioritizing the review and adjudication of background investigations.

Management Response

The Acting CIO concurs with these recommendations. The Acting CIO notes that the Bureau plans to evaluate and leverage potential automated solutions to improve the tracking of all user-access requests and authorizations to Bureau systems. Further, the Acting CIO notes that the Bureau is currently undergoing an internal program review to determine the optimal allocation of resources, as well as defining a prioritization process for the review and adjudication of background investigations.

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.

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. The need for addressing this objective is great, with agencies reporting over 31,000 security incidents to DHS in fiscal year 2018, including web-based attacks,

²⁷ Our audit scope did not include verification of the job functions for these individuals.

phishing attacks, and loss or theft of computing equipment.²⁸ 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.²⁹ 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 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,³⁰ 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.

²⁸ U.S. Government Accountability Office, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545, July 2019.

²⁹ NIST has developed a risk management framework 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. NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*, describes the Risk Management Framework and provides guidelines for applying it to information systems and organizations.

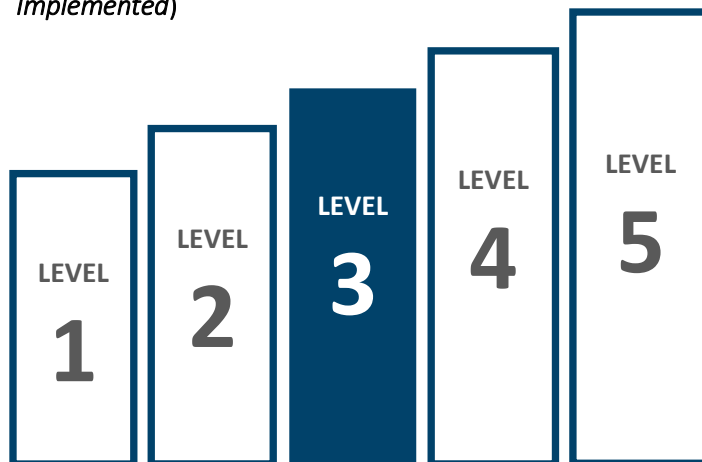
³⁰ 12 U.S.C. §§ 5491(a).

Current Security Posture

The Bureau's data protection and privacy program is operating at a level-3 (*consistently implemented*) maturity, though the agency is also performing remote wiping of mobile devices, which is associated with a higher maturity level (figure 9). The Bureau has also implemented encryption for sensitive data at rest and in transit, as appropriate, and the agency restricts the use of removable storage 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. Further, the privacy team works with IT staff in the Office of Technology and Innovation and other stakeholders as needed for the security of sensitive data. The Bureau has also implemented annual privacy training for all staff and privacy role-based training for individuals with significant privacy-related responsibilities.

Figure 9. Data Protection and Privacy, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

Opportunities for Improvement

Our previously identified issues in the areas of physically securing equipment and inventorying all of the agency's PII continue to represent opportunities for the Bureau to mature its data protection and privacy program. Specifically, in February 2018, we issued a report on the Bureau's privacy program that included two recommendations.³¹ 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 it is stored, and whether a privacy impact assessment or System of Record Notice is required. During our 2018 and 2019 FISMA fieldwork, we found that the Bureau had taken steps to address both of these recommendations. For the recommendation related to the physical security of devices, we found in 2018 that the Bureau had provided new cable locks for equipment, and this year an agency official stated that the Bureau has identified further corrective actions to address the recommendation. Related to the PII inventory recommendation, this year officials informed us that they have identified the divisions that had not been reporting their PII data and that they will have a complete data catalogue in the first quarter of fiscal year 2020. While the Bureau has taken steps to address the two recommendations, all actions have

³¹ 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.

not yet been completed. 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.³²

Further, we identified improvements needed in the Bureau's data exfiltration controls to better ensure the protection of sensitive agency data. Specifically, we found that a technology being used by the Bureau to monitor and control data exfiltration was not consistently implemented across the Bureau's IT environment. For instance, this technology was not blocking access to known internet storage sites and was not deployed across all of the Bureau's network.³³ The Bureau's *Information Security Standards* (CS-S-01) require that the agency monitor and control communications at its external and internal system boundaries and monitor systems to detect unauthorized local, network, and remote connections. In addition, the *FY 2019 CIO FISMA Metrics* highlight the importance of checking outbound communications traffic at external boundaries to detect unauthorized exfiltration of information (for example, anomalous volumes of data, anomalous traffic patterns, elements of PII, and so on) with a solution that is centrally visible at the enterprise level.³⁴

Bureau officials informed us that technical issues have prevented them from deploying their more-effective data exfiltration protections and monitoring across all areas of their environment. Further, Bureau officials stated that they have made a business decision to not block known internet storage sites because of the effect on users' experience in the environment. By ensuring that data exfiltration technologies are deployed consistently across its environment, the Bureau will have greater assurance that sensitive information is not disclosed to those who do not have a need to know.

Recommendation

We recommend that the CIO

5. 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.
 - b. appropriate access to internet storage sites.

Management Response

The Acting CIO concurs with this recommendation and notes that the Bureau will perform a risk assessment to determine the necessary data monitoring and controlling technologies, such as data loss prevention solutions, to be deployed across applicable access points to control the flow of traffic to restricted systems and internet storage sites.

³² After the conclusion of our fieldwork, the Bureau submitted documentation requesting the closure of our PII inventory recommendation. This documentation included an updated PII inventory and standard operating procedure document. We will analyze the steps taken by the Bureau to close this recommendation as part of our audit follow-up process.

³³ The detailed results of our follow-up work in this area will be transmitted to the Bureau under a separate, restricted cover due to the sensitive nature of the information.

³⁴ U.S. Department of Homeland Security, *FY 2019 CIO FISMA Metrics*, Version 1, December 2018.

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* (SP 800-50), 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 ensure that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

A key component of an enterprisewide security training program is the assurance that individuals with significant security responsibilities have the required knowledge, skills, and abilities to perform their roles within the organization. The Federal Cybersecurity Workforce Assessment Act of 2015 requires federal agencies to conduct and report to Congress a baseline assessment of their existing workforce.³⁵ To assist in implementing these requirements, NIST published the *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* (NICE Framework) in August 2017. The framework provides a resource to support a workforce capable of meeting an organization's cybersecurity needs, providing guidance for leaders to better understand, inventory, and track strengths and gaps in their cybersecurity workforce's knowledge, skills, and abilities. Further, the framework organizes individuals with security responsibilities into seven general categories: analyze, collect and operate, investigate, operate and maintain, oversee and govern, protect and defend, and securely provision. These general categories are then associated with specialty areas. Both general categories and specialty areas are used to identify work roles that can be used to tailor training needs for staff, depending on which functions they perform. In addition, NIST guidance identifies that agencies could use a needs assessment to determine their awareness and training needs. NIST SP 800-50 states that a needs assessment can provide justification for management to allocate adequate resources to meet identified awareness and training needs.

In accordance with FISMA requirements, the Bureau's *Cybersecurity Awareness and Training Process* document (CS-P-02) 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.

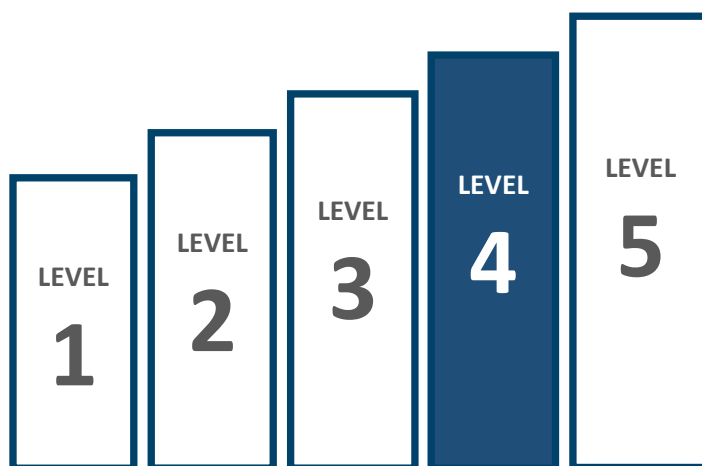
³⁵ Federal Cybersecurity Workforce Assessment Act of 2015, Title III of Pub. L. No. 114-113, 129 Stat. 2242, 2975 (2015) (codified at 5 U.S.C. § 301 note).

Current Security Posture

We found that the Bureau has matured its security awareness and training program from level 3 in 2018 to a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 10). This year, we found that the Bureau has strengthened its cybersecurity training program in several areas. For example, the Bureau leverages an automated security awareness training solution, conducts agencywide phishing campaigns, and provides individuals who have significant security responsibilities with specialized security training before they are provided access to information or perform assigned duties, and periodically thereafter.

Officials stated that these changes are a part of the Bureau's grassroots campaign to increase security awareness throughout the agency. Moreover, in 2019 the Bureau improved its mapping of IT employee types to the respective NICE Framework training category.

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



Source: OIG analysis.

Opportunities for Improvement

While we found that the Bureau's security training program is operating effectively at a level-4 (*managed and measurable*) maturity, we identified opportunities to improve the program. Specially, we found that the Bureau is working on an assessment of the knowledge, skills, and abilities of its workforce, particularly for those individuals with specialized security roles. Completion of this assessment will help the Bureau identify gaps that can be used as a key input to update the agency's awareness and specialized training program. As such, we are not making a recommendation in this area at this time but will continue to monitor the Bureau's progress as part of our future FISMA reviews.

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, maintain knowledge of threats, and ensure security control effectiveness. Examples of the assessment areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Bureau's progress in developing and implementing an ISCM strategy, performing ongoing system authorizations, and using ISCM-related performance measures.

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 an ISCM 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, metrics remain relevant, and data are current and complete.

To further enhance the government's ISCM capabilities, DHS established the CDM program. A key goal of the CDM program is to provide agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential effects, 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 a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 11). The Bureau has made several improvements to its ISCM program. For instance, the agency has enhanced the functionality of its security information and event-monitoring tool by using storyboards to describe attack scenarios and by monitoring for instances of large files being transferred.³⁶ Additionally, the Bureau has implemented continuous monitoring tools that perform spam filtering and vulnerability management for its network devices.

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



Source. OIG analysis.

Opportunities for Improvement

While the Bureau's ISCM program is operating at a level-4 (*managed and measurable*) maturity, we identified opportunities to improve the program. First, as noted earlier in our report, the agency has not established a formal HVA program and identified its HVAs, in accordance with DHS and OMB guidance.

³⁶ Storyboards are attack-based scenarios. The Bureau uses storyboards to describe how alerts from the Bureau's security information and event-monitoring tool are used to detect more-sophisticated attacks using the data already collected by the agency. Because of this new feature, the Bureau has configured more searches within its security information and event-monitoring tool to automatically detect and alert on the storyboards.

Once the Bureau has identified its HVAs, it will need to determine what additional security controls and activities need to be implemented for these systems, including for ISCM. For example, guidance from the Federal CIO Council notes that agencies must implement increased monitoring and analysis of relevant audit logs for all HVAs while maintaining full asset visibility and control. Because our report includes a recommendation for the Bureau to establish an overall HVA program to include specific control considerations for HVAs, we are not making a separate recommendation in this area. We will continue to monitor the Bureau's efforts to determine control requirements for its HVAs, including for ISCM, as part of our future FISMA reviews.

Second, the Bureau is integrating its ISCM strategy and supporting processes with its ERM program. As noted earlier, the Bureau has not implemented all components of its ERM program, including defining its risk appetite statement and tolerance levels. We believe that as the Bureau continues to mature its ERM program, updates will be needed to the agency's ISCM program to ensure alignment, particularly with respect to monitoring frequencies and metrics. For example, SP 800-137 notes that an organization's ISCM strategy is developed and implemented to support risk management, in accordance with organizational risk tolerance. Further, SP 800-137 states that metrics are designed and ISCM frequencies are determined to ensure that information needed to manage risk within organizational tolerances is available. Because the Bureau is implementing its ERM program, we are not making a specific recommendation in this area at this time. We will continue to monitor the Bureau's efforts to update its ISCM program to better align with ERM activities as part of our future FISMA reviews.

Finally, the Bureau could mature its ISCM program by using the tools and capabilities offered by the CDM program, where appropriate. Bureau officials stated that they are still working with DHS to integrate their ISCM tools with those offered under the CDM program. Bureau officials further stated that network connections will be established to initiate data feeds between the two agencies. Because the Bureau is relying on the milestones established by DHS for CDM implementation for small agencies, we will not make a recommendation in this area at this time. However, we will continue to monitor the Bureau's progress in implementing the capabilities of the CDM program as part of our future FISMA reviews.

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. Examples of the assessment areas in this security function, as outlined in the 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 notes that an incident response process consists of four main phases: preparation; detection and analysis; containment, eradication, and recovery; and postincident activity (table 5). 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 5. 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 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 in support of incident response, including reporting incidents to the United States Computer Emergency Readiness Team within an hour as required by the *US-CERT Federal Incident Notification Guidelines*.

Current Security Posture

We found that the Bureau’s incident response program continues to operate at a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 12). This year, the Bureau matured several incident response capabilities. For instance, the agency has deployed a data loss prevention tool, and it is using a service offered by DHS for preventing malicious traffic from affecting the agency’s network. Further, since our review last year, the Bureau has begun tracking additional metrics related to the

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



Source. OIG analysis.

effectiveness of incident response processes and has created plans to further mature capabilities in this area.

Opportunities for Improvement

While the Bureau's incident response program is operating at a level-4 (*managed and measurable*) maturity, we identified opportunities to improve the program by ensuring the accuracy and consistency of cybersecurity and privacy event information captured in incident tickets. The Bureau uses tickets as the primary vehicle for documenting the characteristics of cybersecurity and privacy events and for ensuring that such events are routed to appropriate individuals for action, including the determination of whether events constitute an incident. Cybersecurity events can be generated from a number of sources, such as monitors and host-based sensors placed on the Bureau's network; internal and external logs; and reporting of suspicious activity, such as emails, by end users. Specifically, we found that internal categorization³⁷ of cybersecurity and privacy events was not accurately or consistently performed in incident tickets. Further, for privacy events, we identified multiple instances where the *date closed* field was left blank in incident tickets. Because of the sensitive nature of this information, the details of these issues will be transmitted to the Bureau under a separate, restricted cover.

Bureau officials noted that they employ a peer review process for cybersecurity incident tickets that should have flagged the issues we identified. Additionally, Bureau officials stated that for privacy incident tickets, personnel turnover in early 2019 contributed to the completeness issues we identified. The Bureau's *Information Security Standards* (CS-01) requires that information system security incidents be tracked and documented and that metrics be used for measuring the incident response capability within the organization. Ensuring the accuracy of information captured in security and privacy incident tickets could provide the Bureau with additional assurance that such incidents are effectively investigated and reported. In addition, the Bureau will have more accurate and comprehensive information for its incident response metrics and trend analyses.

Recommendation

We recommend that the CIO and the Chief Data Officer

6. Ensure that data captured in security and privacy incident processes and tickets are accurate, consistent, and of high quality.

Management Response

The Acting CIO concurs with this recommendation. The Acting CIO notes that the Bureau plans to make improvements in its privacy event and incident ticketing practices by performing a review of internal categorization practices to improve data quality and ensure enhanced risk mitigation ability. The Acting CIO further notes that the agency is monitoring data quality metrics and plans to make improvements to those metrics to minimize the likelihood of data quality issues occurring in the future.

³⁷ The Bureau's *Computer Security Incident Response Team (CSIRT) Standard Operating Procedures* notes that event categories can include denial of service, misuse, lost device, PII spillage, and suspicious email.

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.

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. The IG FISMA reporting metrics focus on evaluating agency contingency planning processes. Examples of the assessment areas in this security function that we assessed include the Bureau's processes for conducting business impact analysis (BIA), developing and testing information system contingency plans, and managing 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.

SP 800-34 notes that conducting a 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.

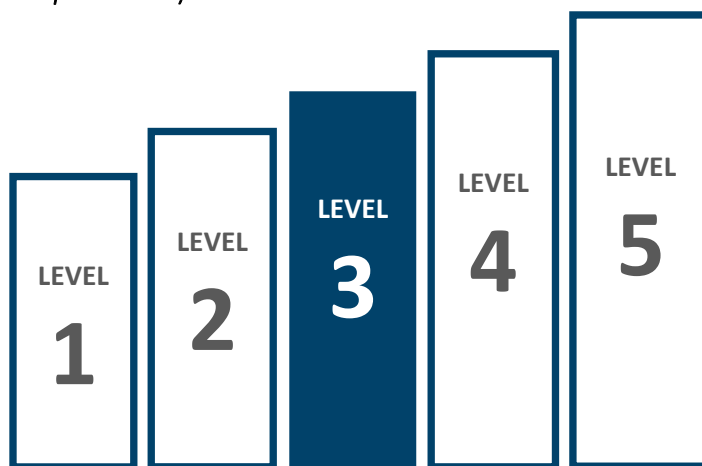
Another key component of an effective contingency planning program is the consideration of risk from an organization's ICT supply chain. NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (SP 800-161), highlights ICT supply chain concerns associated with contingency planning, including alternative suppliers of system components and services, denial-of-service attacks to the supply chain, and alternate delivery routes for critical system

components.³⁸ 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 the procurement of IT and to establish criteria for determining which types of products pose supply chain security risks to the federal government.³⁹ 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.⁴⁰ For example, with respect to contingency planning, the framework notes that response and recovery planning and testing should be conducted with suppliers and third-party providers.

Current Security Posture

The Bureau's contingency planning program is operating at a level-3 (*consistently implemented*) maturity (figure 13). For instance, the Bureau has defined and communicated roles and responsibilities for contingency planning and reinforces these during newly implemented functional testing. Additionally, the Bureau has conducted an organizational-level (process-focused) BIA to determine contingency planning requirements and priorities.

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



Source. OIG analysis.

Opportunities for Improvement

We identified opportunities for the Bureau to mature its contingency planning program in the areas of system-level BIAs, contingency plan testing, and consideration of ICT supply chain risks. Specifically, while the Bureau has completed an organizational-level BIA, the organization has not completed system-level BIAs. NIST SP 800-34 notes that system-level BIAs should include determination of process and system criticality, outage impacts, and estimated downtime (including maximum tolerable downtime, recovery time objective, and recovery point objective), resource requirements, and recovery priorities for system resources. Bureau officials stated that they believe that the key components of a system-level BIA are included in their *Information Technology Contingency Plan* (CS-PL-01). However, we found that the plan does not cover system criticality, outage impacts, recovery priorities, and other key timings for the organization's systems. By

³⁸ The guidance and controls in this 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.

³⁹ At the conclusion of our fieldwork, the Federal Acquisition Security Council had not yet issued guidance related to mitigation of ICT supply chain risks.

⁴⁰ National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.

conducting system-level BIAs, the Bureau will be able to identify critical services within each system and adjust contingency planning priorities and resources, as appropriate.

We also found that the Bureau has opportunities to mature its contingency planning program through the consideration and management of ICT supply chain risks. SP 800-161 notes that many techniques used for contingency planning, such as alternative processing sites, have their own ICT supply chains and risks. Organizations should ensure that they understand and manage ICT supply chain risks and dependencies related to the contingency planning activities, as necessary. While we recognize that SP 800-161 applies to high-risk systems, with the additional governmentwide focus on supply chain risk management, we believe that the Bureau should determine the applicability of ICT supply chain risks to its environment. As the Federal Acquisition Security Council works to develop additional criteria regarding the supply chain security risks to the federal government, the Bureau has an opportunity to further enhance its contingency planning program through the consideration of these risks. While we are not making a recommendation in this area at this time, we will continue to monitor the Bureau's efforts, including its response to guidance issued by the Federal Acquisition Security Council, as part of our future FISMA reviews.

Recommendation

We recommend that the CIO

7. Ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.

Management Response

The Acting CIO concurs with this recommendation. The Acting CIO notes that the Bureau will continue to mature its contingency management program to encompass system-level BIA, as appropriate. The Acting CIO further notes that this effort will take into consideration additional contingency planning processes, such as determination of system criticality, outage impacts, estimated downtime, resource requirements, and recovery priorities.

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.



Status of Prior Years' Recommendations

As part of our 2019 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 2019 FISMA audit (table 6). Based on corrective actions taken by the Bureau, we are closing 3 prior recommendations related to data protection and privacy, incident response, and contingency planning. The remaining 7 recommendations related to risk management, configuration management, and identity and access management will remain open. We will update the status of these recommendations in our upcoming semiannual report to Congress and continue to monitor the Bureau's progress in addressing our open recommendations as a part of our future FISMA reviews.

Table 6. Status of Prior Years' Recommendations

| Recommendation | Status | Disposition |
|--|--------|---|
| Risk management | | |
| In our 2016 FISMA audit report, we recommended that the CIO, in conjunction 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 data loss prevention. | Open | The Bureau has developed a communications plan to raise organizational awareness about insider threats. The plan defines organization structures and outlines the current capabilities that support the insider threat program from a people, processes, and technology perspective. However, the Bureau has not fully implemented its data loss prevention tool. |
| 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 yet finalized its risk appetite statement or risk tolerance levels. |

| Recommendation | Status | Disposition |
|--|--------|---|
| 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. |
| In our 2018 FISMA audit report, we recommended that the CIO strengthen configuration management processes by (1) remediating configuration-related vulnerabilities in a timely manner and (2) ensuring that optimal resources are allocated to perform vulnerability remediation activities. | Open | The Bureau still has numerous critical and high-risk vulnerabilities that were not remediated in a timely manner. Further, our operating system-level scanning identified a number of critical and high-risk vulnerabilities that had also been identified by the Bureau's internal vulnerability scans months earlier. |
| In our 2018 FISMA audit report, we recommended that the CIO develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones. | Open | Bureau officials informed us that they are updating policy and implementing a tool to enforce the application of current patches for mobile phones. |
| Identity and access 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 implemented several technical solutions that in totality did not completely meet NIST level of assurance 4 multifactor authentication. |
| In our 2018 FISMA audit report, 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 access agreements and associated rules of behavior are completed prior to access being granted to systems. |

| Recommendation | Status | Disposition |
|--|--------|--|
| Data protection and privacy | | |
| In our 2018 FISMA audit report, we recommended that the CIO ensure that the Bureau's existing ISCM approach is implemented for an internal collaboration tool to appropriately restrict and monitor access. | Closed | The Bureau has taken actions to strengthen the security of its internal collaboration tool, including using continuous monitoring processes to restrict access and monitor logs. |
| 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. | Closed | The Bureau has ensured that logs from its cloud computing environment are uploaded to its central automated solution. |
| Contingency planning | | |
| In our 2016 FISMA audit report, we recommended that the CIO strengthen the Bureau's contingency program by performing an agencywide BIA and updating the agency's continuity of operations plan and IT contingency plan to reflect the results of the BIA and the current operating environment of the Bureau. | Closed | The Bureau conducted an organizational-level BIA and updated its strategy and planning documentation accordingly. |



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 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 interviewed Bureau management and staff; analyzed security policies, procedures, and documentation; performed vulnerability scanning at the network, operating system, and database levels for select systems;⁴¹ and observed and tested specific security processes and controls. We used commercially available software to perform data analytics to support our effectiveness conclusions for specific metrics in multiple security domains. The data we analyzed were related to three of the Bureau's 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 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 2019 to September 2019. 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.

⁴¹ The detailed results of our technical testing will be transmitted to the Bureau under a separate, restricted cover due to the sensitive nature of the information.

Appendix B: Management Response

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

October 23, 2019

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 *2019 Audit of the Bureau's Information Security Program*. We are pleased that you found that 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) 2020, the Bureau will continue to enhance its processes and technologies to continue to raise its overall maturity level 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 has matured its Risk Management program from level-3 maturity (in FY 2018) to level-4 maturity (*managed and measurable*) in FY 2019. The Bureau employs automation to track the life cycle of its hardware assets. Additionally, the Bureau maintains qualitative and quantitative performance measures related to its plans of action and milestones process. In FY 2020, the Bureau will continue to improve its risk management program by defining the risk appetite statement and tolerance levels and continue to implement its data loss prevention tool across the enterprise.

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. Additionally, the Bureau tracks and reports on performance measures related to its change control activities. In FY 2020, the Bureau will continue to improve its configuration management program by prioritizing the implementation of an automated solution and process to assess and manage database security configurations as well as implementing a process to ensure timely application of patches and security updates.

consumerfinance.gov

- The Bureau's Identity and Access Management (ICAM) program is operating at level-3 maturity (*consistently implemented*). The Bureau has strengthened identity and access controls for its remote access program and is utilizing enhanced features offered by its security information, event monitoring, and antivirus software to perform more detailed user-activity reviews for remote access sessions. In FY 2020, the Bureau plans to improve its identity and access management program by refining the process of maintaining user access forms and prioritizing the adjudication of background investigations.
- The Bureau's Data Protection and Privacy program is operating at level-3 maturity (*consistently implemented*), with the Bureau performing remote wiping of mobile devices, which is associated with a higher level of maturity. 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 addition, the Bureau has established and maintains a privacy program to provide for the development and maintenance of privacy controls. The Bureau has also implemented annual privacy training for all staff and privacy role-based training for individuals with significant privacy-related responsibilities. In FY 2020, the Bureau will continue improving its data protection and privacy program by consistently deploying exfiltration tools across the enterprise to monitor and prevent exfiltration of data to unauthorized sites and systems.
- The Bureau's Security Training and Awareness program is operating at level-4 maturity (*managed and measurable*). The Bureau has matured its security awareness and training program from level-3 maturity (in FY 2018) to level-4 maturity (*managed and measurable*). The Bureau has strengthened its cybersecurity training program in several areas, such as leveraging an automated security awareness training solution, conducting Bureau-wide phishing campaigns, and providing specialized training to individuals with significant security responsibilities. In FY 2020, the Bureau plans to improve its security training and awareness program by performing a knowledge, skills, and abilities assessment of its entire workforce. The results of the assessment will help the Bureau identify gaps and will be used to improve the Bureau's security training and awareness program.

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

- The Bureau's Information Security Continuous Monitoring (ISCM) program continues to operate at level-4 maturity (*managed and measurable*). The Bureau has made several improvements to its ISCM program, including the enhanced functionality of its security information and event monitoring tool by using storyboards to describe attack scenarios and by monitoring for instances of large files being transferred. Additionally, the Bureau has implemented continuous monitoring tools that perform spam filtering and vulnerability management for its network devices. In FY 2020, the Bureau will improve its ISCM program by enhancing security controls of the Bureau's identified High Value Asset (HVA) and implementation of real-time monitoring of controls.

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 matured several incident response capabilities. The Bureau has deployed a data loss prevention tool, and it is using a service offered by DHS for preventing malicious traffic from affecting the Bureau's network. 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 FY 2020, the Bureau will improve its incident response program by reviewing the Bureau's categorization process of cybersecurity and privacy event information captured in incident response tickets to improve data accuracy and consistency. In addition, the Bureau will begin integrating behavioral data analytics and workflow automation into its centralized audit log collection system.

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 defined and communicated roles and responsibilities for contingency planning and reinforces these during newly implemented functional testing. Additionally, the Bureau has conducted an organizational-level (process-focused) Business Impact Analysis (BIA) to determine contingency planning requirements and priorities. In FY 2020, the Bureau will improve its contingency planning program by prioritizing the development of system-level 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,

KATHERINE SICKBERT
Digitally signed by
KATHERINE SICKBERT
Date: 2019.10.23
14:51:59 -04'00'

Katherine Sickbert
Acting Chief Information Officer

**Response to recommendations presented in the Draft OIG Report,
“2019 Audit of the Bureau’s Information Security Program.”**

Recommendation 1: Determine which components of an HVA program are applicable to the Bureau and ensure that, if appropriate, a governance structure and implementation of HVA-specific baselines, planning activities, and enhanced controls for agency HVAs are established with regard to information security, privacy, and ERM.

Management Response: The Bureau concurs with this recommendation. The Privacy and Cybersecurity Teams will lead the coordination effort to review how an HVA program may apply to the Bureau to ensure resulting Bureau governance processes incorporate related activities, such as identification of HVA and applicable controls or processes, into enterprise risk management (ERM).

Recommendation 2: Ensure that established security assessment and authorization processes are performed prior to the deployment of all cloud systems used by the Bureau.

Management Response: The Bureau concurs with this recommendation. The Cybersecurity Team is actively working to decommission the identified, deployed cloud system. Moving forward, all Bureau systems will thoroughly undergo the Security Assessment and Authorization processes before being deployed for production use.

Recommendation 3: Ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonprivileged users.

Management Response: The Bureau concurs with this recommendation. The Bureau plans to evaluate and leverage potential, automated solutions to improve the tracking of all user-access requests and authorization to Bureau systems.

Recommendation 4: Conduct a comprehensive, risk-based review to determine the optimal resources and process for prioritizing the review and adjudication of background investigations.

Management Response: The Bureau concurs with this recommendation. The Office of Security Programs is currently undergoing an internal program review to determine the optimal allocation of resources, as well as a defining a prioritization process for the review and adjudication of background investigations.

Recommendation 5: Perform a risk assessment of the Bureau’s technology for monitoring and controlling data exfiltration to ensure that the technology is consistently deployed across all access points to the Bureau’s environment and that access to Internet storage sites is determined by the risk-based review.

Management Response: The Bureau concurs with this recommendation. The Bureau will perform a risk assessment to determine the necessary data monitoring and controlling technologies, such as Data Loss Prevention solutions, to be deployed across applicable access points to control the flow of traffic to restricted systems and Internet storage sites.

Recommendation 6: Conduct a review of the current security and privacy incident processes as well as past tickets to ensure data captured are accurate, consistent, and high-quality records to allow mitigation of issues, enhancement of process flows and mitigation of any resulting impacts.

Management Response: The Bureau concurs with this recommendation. The Privacy Team plans to make improvements in its privacy event and incident ticketing practices by performing a review of internal categorization practices to improve data quality and ensure enhanced risk mitigation ability. The Cybersecurity Team has and will continue taking additional steps to ensure data accuracy. The Cybersecurity Team is currently monitoring data quality metrics and plans to make improvements of those metrics to minimize the likelihood of data quality issues occurring in the future.

Recommendation 7: Ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.

Management Response: The Bureau concurs with this recommendation. As described in NIST Special Publication 800-34, Revision 1 (SP 800-34), Contingency Planning Guide for Federal Information Systems, the Bureau will continue to mature its contingency management program to encompass system-level Business Impact Analysis, as appropriate, considering additional contingency planning such as the determination of process and system criticality, outage impacts, estimated downtime, resource requirements, and recovery priorities for system resources.



Abbreviations

| | |
|--------------------------|---|
| ATO | authorization to operate |
| BIA | business impact analysis |
| Bureau | Bureau of Consumer Financial Protection |
| CDM | Continuous Diagnostics and Mitigation |
| CIO | Chief Information Officer |
| DHS | U.S. Department of Homeland Security |
| ERM | enterprise risk management |
| FedRAMP | Federal Risk and Authorization Management Program |
| 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 |
| NICE Framework | <i>National Initiative for Cybersecurity Education Cybersecurity Workforce Framework</i> |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| PII | personally identifiable information |
| PIV | personal identity verification |
| SA&A | security assessment and authorization |
| SECURE Technology Act | Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2018 |
| SP 800-34 | Special Publication 800-34, Revision 1, <i>Contingency Planning Guide for Federal Information Systems</i> |
| SP 800-39 | Special Publication 800-39, <i>Managing Information Security Risk: Organization, Mission, and Information System View</i> |
| SP 800-50 | Special Publication 800-50, <i>Building an Information Technology Security Awareness and Training Program</i> |

| | |
|-------------------|--|
| SP 800-53 | Special Publication 800-53, Revision 4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i> |
| SP 800-122 | Special Publication 800-122, <i>Guide to Protecting the Confidentiality of Personally Identifiable Information</i> |
| SP 800-137 | Special Publication 800-137, <i>Information Security Continuous Monitoring for Federal Information Systems and Organizations</i> |
| SP 800-161 | Special Publication 800-161, <i>Supply Chain Risk Management Practices for Federal Information Systems and Organizations</i> |

Report Contributors

Khalid Hasan, Senior OIG Manager
Andrew Gibson, OIG Manager
Jeff Woodward, Senior IT Auditor
Kaneisha Johnson, IT Auditor
LaToya Holt, Senior Auditor
Emily Martin, IT Auditor
Justin Byun, IT Audit Intern
Fay Tang, Statistician
Alexander Karst, Senior Information Systems Analyst
Peter Sheridan, Assistant 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