Audit Report
2021-IT-C-015
October 29, 2021

Bureau of Consumer Financial Protection

2021 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

Executive Summary, 2021-IT-C-015, October 29, 2021

2021 Audit of the Bureau's Information Security Program

Findings

The Bureau of Consumer Financial Protection's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, we found that the Bureau has taken several steps to strengthen its information security program. For instance, the agency has leveraged its information security training skills assessment to identify improvements needed in staffing levels. Further, the Bureau continues to capture and report incident response metrics and is evaluating the use of automation to strengthen ticketing processes.

We identified opportunities for the Bureau to strengthen its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five National Institute of Standards and Technology Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. Specifically, we identified opportunities to improve the Bureau's organizationwide cybersecurity risk management processes through the use of a cybersecurity risk register process. We also found that the Bureau was not ensuring that specific technical vulnerabilities were appropriately tracked in a plan of actions and milestones. In addition, we found that the Bureau had not updated its configuration management plan to reflect new technologies and processes.

In addition, the Bureau has taken sufficient actions to close 2 of the 11 recommendations from our prior FISMA audit reports that were open at the start of this audit. The closed recommendations relate to the implementation of mobile device management technologies and completion of a business impact analysis for information technology systems. We are leaving open 9 recommendations related to risk management, configuration management, data protection and privacy, and identity and access management. We will update the status of these recommendations in our spring 2022 semiannual report to Congress and continue to monitor the Bureau's progress as part of future FISMA audits.

Recommendations

This report includes three new recommendations designed to strengthen the Bureau's information security program in the areas of risk and configuration management. 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 FISMA audits.

Purpose

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

Background

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

Recommendations, 2021-IT-C-015, October 29, 2021

2021 Audit of the Bureau's Information Security Program

Number	Recommendation	Responsible office
1	Develop and implement a cybersecurity risk register and associated process to identify and manage organizationwide cybersecurity risks.	Office of Technology and Innovation
2	Strengthen oversight processes to ensure, as appropriate, that weaknesses identified through vulnerability scanning activities are being managed through the agency's POA&M process.	Office of Technology and Innovation
3	Ensure that the Bureau's configuration management plan is updated to reflect current processes, procedures, and technologies.	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 29, 2021

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2021-IT-C-015: *2021 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). Specifically, FISMA 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, performed data analytics, and conducted technical testing. We will use the results of this audit to respond to specific questions in the U.S. Department of Homeland Security's *FY 2021 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 C to our report.

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

cc: Tiina Rodrigue
Tannaz Haddadi
Marianne Roth
Dana James
Lauren Hassouni
Anya Veledar
Carlos Villa

Distribution:
Chris Chilbert, Chief Information Officer
Martin Michalosky, Chief Administrative Officer
Ren Essene, Chief Data Officer

Contents

Introduction

Objectives

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

Background

FISMA requires agencies to develop, document, and implement an agencywide security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or another source.[1] FISMA also requires that each inspector general (IG) perform an annual independent evaluation to determine the effectiveness of the information security program and practices of their respective agency, including testing the effectiveness of information security policies, procedures, and practices for select systems.

To support independent evaluation requirements, the U.S. Department of Homeland Security (DHS) publishes FISMA reporting metrics for IGs to respond to on an annual basis. The *FY 2021 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 nine 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]

As noted in DHS's *FY 2021 IG FISMA Reporting Metrics*, one of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving outcomes that strengthen federal cybersecurity, including implementation of the administration's priorities and best practices. One such area is increasing the maturity of the federal government's supply chain risk management (SCRM) practices. As such, DHS's *FY 2021 IG FISMA Reporting Metrics* includes a new domain on SCRM within the *identify* function, focusing on the maturity of agency SCRM strategies, plans, policies, and processes.[4]

[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 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, May 12, 2021.

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

[4] This new domain on SCRM references criteria in NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53, Rev. 5). As noted in the *FY 2021 IG FISMA Reporting Metrics*, to provide agencies with sufficient time to implement requirements from Special Publication 800-53, Revision 5, these new metrics are not being considered for the purposes of the *identify* function maturity rating in 2021.

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

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

Source: U.S. Department of Homeland Security, *FY 2021 IG FISMA Reporting Metrics*.

FISMA Maturity Model

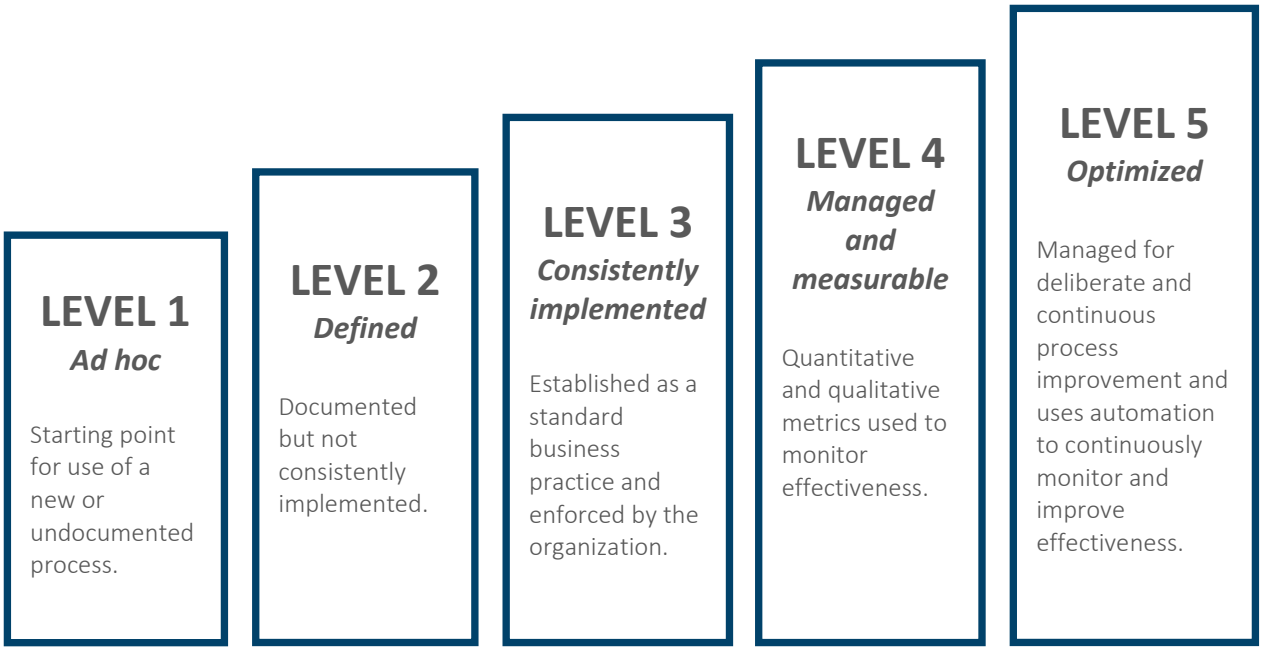
FISMA requires that IGs assess the effectiveness of information security controls that support the operations and assets of their respective agency. To that end, the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Office of Management and Budget, DHS, and other 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 (1) to summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) to provide transparency to agency chief information officers (CIOs), top management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and (3) to help ensure that annual FISMA reviews are consistent across IGs.

The five levels of the IG FISMA maturity model are

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

The foundational levels (1–3) of the model are geared toward the development and implementation of policies and procedures, and the advanced levels (4–5) capture the extent to which agencies institutionalize those policies and procedures (figure 1). The maturity levels of each of the security domains will dictate the overall maturity of an organization's information security program. As noted in DHS's *FY 2021 IG FISMA Reporting Metrics*, level 4 (*managed and measurable*) represents an effective level of security.[5] Details on the scoring methodology for the maturity model are included in appendix A.

Figure 1. FISMA Maturity Model Rating Scale



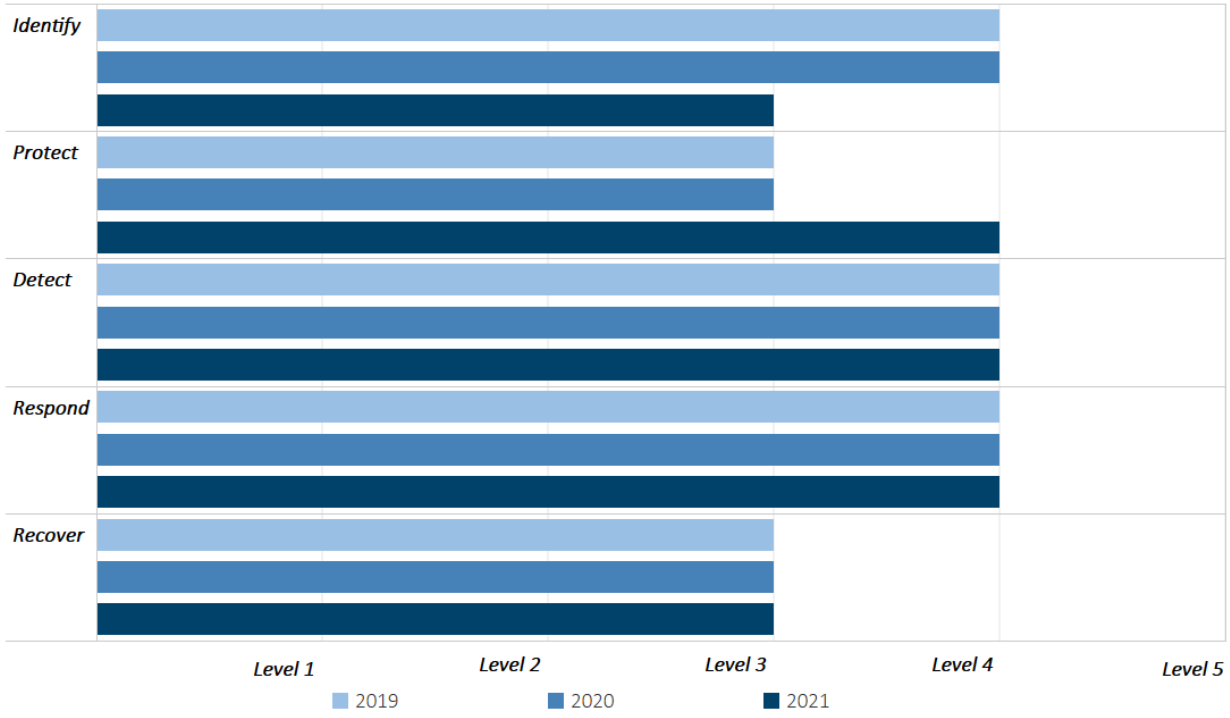
Source: OIG analysis of DHS's *FY 2021 IG FISMA Reporting Metrics*.

[5] NIST defines *security and privacy 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 designated security and privacy requirements. National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 5, updated December 10, 2020.

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

We found that the Bureau's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 2).[6] Although the Bureau has strengthened its program since our 2020 FISMA report, the agency has opportunities to further mature its processes across specific FISMA domains in all five NIST Cybersecurity Framework security functions: *identify*, *protect*, *detect*, *respond*, and *recover*.

Figure 2. Maturity of the Bureau's Information Security Program, by Security Function, 2019–2021



Source: OIG analysis.

For the *identify* function, the Bureau has decreased in maturity to level 3 (*consistently implemented*) because of two key reasons. First, we found that the agency is not using a cybersecurity risk register process to identify and prioritize its organizationwide security and privacy risks. Such a process could be used to aggregate, normalize, and prioritize risk responses across the agency. Secondly, we found that the

[6] To determine the maturity of the Bureau's information security program, we used the scoring methodology outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*. Appendix A provides additional details on the scoring methodology.

Bureau was not ensuring that technical system-level vulnerabilities open beyond 60 days were being tracked as part of the agency's plan of action and milestones (POA&M) process.

While we found that the *protect* function increased to a level-4 (*managed and measurable*) maturity this year, we identified an opportunity to strengthen configuration management activities. Specifically, we noted that the Bureau's configuration management plan is outdated and does not reflect new technologies and processes.

In addition, we found that the Bureau has taken sufficient actions to close two recommendations from our previous FISMA audit reports related to patching mobile devices and completing system-level business impact analyses (BIAs). We are leaving open nine recommendations related to risk management, configuration management, identity and access management, and data protection and privacy from our previous FISMA audit reports and will continue to monitor the Bureau's actions in these areas as part of our future FISMA audits.

Identify

The objective of the *identify* function in NIST's Cybersecurity Framework is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities. The Cybersecurity Framework highlights risk management processes that organizations can implement to inform and prioritize decisions. Examples of the areas in this security function, as outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*, that we assessed include the Bureau's processes for cybersecurity risk management, enterprise architecture, asset management, POA&Ms, and SCRM.

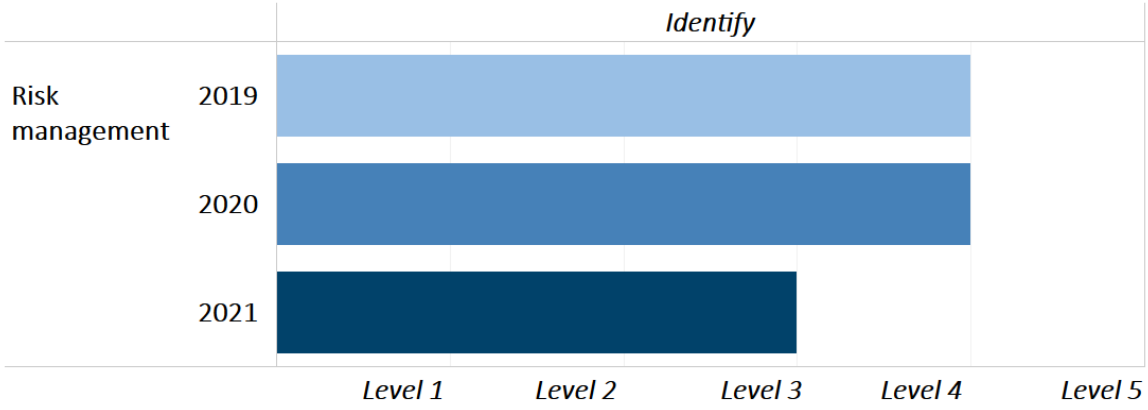
Risk Management

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. *Cybersecurity risk management* refers to the full range of activities undertaken to protect information technology (IT) and data from unauthorized access and other cyberthreats; maintain awareness of cyberthreats; detect anomalies and incidents adversely affecting IT and data; and mitigate the impact of, respond to, and recover from incidents.

Current Agency Maturity

As shown in figure 3, we found that the Bureau's risk management program decreased in maturity from the previous year and is operating at level 3 (*consistently implemented*).

Figure 3. Maturity of the Risk Management Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Bureau continues to implement its risk management processes. Specifically, we noted that the agency

- updated its risk management policies and procedures
- developed a risk appetite statement
- continues to use a tool to support centralized hardware asset management
- maintains qualitative and quantitative performance measures related to its POA&M process

We have two recommendations in the risk management domain from our previous FISMA audit reports that remain open. These recommendations relate to finalizing enterprise risk tolerances and ensuring that security assessment and authorization processes are completed for cloud systems before deployment. The status of prior FISMA recommendations is detailed in appendix B.

Opportunities for Improvement

To mature the Bureau's risk management program and ensure that it is effective, we identified two areas for improvement. The first area relates to using a cybersecurity risk register process to identify and prioritize organizationwide cybersecurity and privacy risks. The second area relates to ensuring that technical system-level vulnerabilities open beyond 60 days are managed as part of the Bureau's POA&M process.

Organizationwide Cybersecurity Risk Assessment and Risk Register

We found that while the Bureau has processes in place to assess and manage system-level risks, the agency can improve its ability to identify and manage cybersecurity risks from an organizational perspective. Specifically, the Bureau performs several system-level cybersecurity risk management activities, such as security planning, authorization, and vulnerability scanning. However, the agency does not have an effective process to analyze and normalize this information and identify organization-level risks. We believe that a key cause for this issue is that the Bureau has not developed a cybersecurity risk register process to provide an organizationwide view of system-level risks. Further, the Bureau is still in the process of implementing an enterprise risk management (ERM) program, and we have an open recommendation in this area. See appendix B for further information on the status of this

recommendation. Bureau officials informed us that they are creating a cybersecurity risk register process and have procured a tool to assist in this area. Bureau officials plan to implement the tool in 2022.

NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, requires organizations to conduct enterprisewide security and privacy risk assessments on an ongoing basis.[7] Specifically, the publication notes that risk assessment at the organizational level leverages aggregated information system-level risk assessments, continuous monitoring, and any strategic risk considerations relevant to the organization. NIST Interagency/Internal Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*,[8] highlights the importance of using a cybersecurity risk register as part of an organizationwide security risk assessment. Specifically, the publication notes that it is necessary to have a comprehensive set of risks and to record them in a risk register. The publication also notes that using a cybersecurity risk register provides consistency in capturing and communicating risk-related information (including risk response) throughout the ERM process. We believe that establishing a cybersecurity risk register process could help ensure that the Bureau identifies and prioritizes enterprisewide security and privacy risks.

System-Level POA&Ms

While the Bureau has established a POA&M process to ensure that appropriate remedial actions are taken to address vulnerabilities, we found that the process was inconsistently implemented for weaknesses identified through the agency's internal vulnerability scanning. Specifically, the Bureau performs routine vulnerability scanning of its IT infrastructure.[9] We found that POA&M items were not consistently created for systems with vulnerabilities that were open longer than 60 days. We also noted that a fix was available for these vulnerabilities for over 60 days.

The Bureau's *POA&M Management Process* states that a POA&M item for the vulnerability scanning control, RA-5, must be created if a system has vulnerabilities open for longer than 60 days when a patch is available for over 60 days. The Bureau's *POA&M Management Process* also notes that vulnerability scanning items can be grouped into one entry under RA-5. However, we could not verify whether open vulnerabilities were being grouped appropriately. We also reviewed other controls listed on the POA&Ms for Bureau systems but did not identify enough entries to cover the vulnerabilities identified through scanning.

We believe that a key cause for this issue is that the Bureau's POA&M oversight processes do not include steps to effectively identify and monitor technical vulnerabilities that are open for longer than 60 days and that have a fix available. In addition, according to agency officials, vulnerabilities could be bundled for some systems or could be under a control other than RA-5; however, creating POA&Ms under controls other than RA-5 is inconsistent with the Bureau's POA&M policy requirement. By ensuring that technical

---

[7] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, Revision 2, December 2018.

[8] NIST Interagency/Internal Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, October 2020.

[9] *Vulnerability scanning* commonly refers to using automated tools to identify hosts and host attributes (for example, operating systems, applications, and ports). Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations and can help validate compliance with or deviations from an organization's security policy.

scanning vulnerabilities, as necessary, are tracked in a POA&M, the Bureau will be better able to ensure timely mitigation.

Recommendations

We recommend that the CIO

1. Develop and implement a cybersecurity risk register and associated process to identify and manage organizationwide cybersecurity risks.

2. Strengthen oversight processes to ensure, as appropriate, that weaknesses identified through vulnerability scanning activities are being managed through the agency's POA&M process.

Management Response

The CIO concurs with our recommendations. In his response, the CIO states that in fiscal year 2021, the Office of Technology and Innovation (T&I) implemented a risk management program that established risk profiles for T&I, which included a cybersecurity risk profile, to document major IT risks. The CIO further states that the Bureau's Office of Cybersecurity will leverage the existing cybersecurity risk register to coordinate with the Bureau's and T&I's risk management programs on implementing an escalation process that aggregates information systems, business processes, and enterprise-level risks.

In addition, the CIO states that the Office of Cybersecurity is updating POA&M processes to create POA&M items for weaknesses identified through vulnerability scanning activities in accordance with vulnerability criticality and remediation thresholds. This activity is scheduled to be updated by the fourth quarter of fiscal year 2022.

OIG Comment

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

Supply Chain Risk Management

FISMA, as amended by the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act,[10] requires agencies to develop an overall risk management strategy, implementation plan, and policies and processes to govern SCRM activities.[11] The importance of SCRM is also highlighted in Executive Order 14028, *Improving the Nation's Cybersecurity*, which states that the federal government must take action to rapidly improve the security and integrity of the software supply chain.[12] In support of this goal, Executive Order 14028 tasks NIST, the Office of Management and Budget, and other federal

[10] Strengthening and Enhancing Cyber-capabilities by Utilizing risk Exposure Technology Act of 2018, Pub. L. No. 115-290, 132 Stat. 5173 (2018) (codified at 41 U.S.C. §§ 1321–4713).

[11] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, Revision 2, December 2018, defines *SCRM* as the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.

[12] Exec. Order No. 14028 (May 12, 2021).

agencies to issue guidance on various elements of SCRM, such as secure software development, use of encryption, and maintenance of accurate and up-to-date information on the origin of software code or components.[13]

As noted earlier, SCRM is a new domain included in DHS's *FY 2021 IG FISMA Reporting Metrics.* This new domain focuses on the maturity of an agency's SCRM strategies, plans, policies, and processes and references criteria in NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53, Rev. 5).[14] As noted in the *FY 2021 IG FISMA Reporting Metrics*, to provide agencies with sufficient time to implement requirements from NIST SP 800-53, Rev. 5, these new metrics are not being considered for the purposes of the *identify* function maturity rating in 2021. As such, while we are not providing an overall maturity rating this year for the Bureau's SCRM program, we highlight the steps the agency has taken in this area and additional improvements we believe are needed. We will continue to monitor and report on the maturity of the Bureau's SCRM program and processes as part of our future FISMA audits.

Current Agency Maturity

In September 2021, the Bureau finalized a standard operating procedure document titled *Cybersecurity Supply Chain Risk Management (C-SCRM) Process*.[15] This document includes processes used by the Bureau's Office of Cybersecurity to manage cybersecurity-related supply chain risks within the agency's IT environment and perform

- research and analysis before the procurement of new IT hardware and software
- ongoing monitoring of vendors' security performance within the Bureau's IT environment[16]

In addition, the Bureau's information security program and supporting policies and procedures address various components of SCRM, such as risk management activities and security control requirements for the Bureau's use of third-party providers.

[13] This guidance was not finalized at the time of our fieldwork.

[14] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, updated December 2020.

[15] Standard Operating Procedure TI-P-40-009, *Cybersecurity Supply Chain Risk Management (C-SCRM) Process*, September 16, 2021.

[16] This document was finalized after the conclusion of our fieldwork. As such, we plan to assess its implementation and effectiveness as part of our future FISMA audits.

Opportunities for Improvement

As further governmentwide policies, standards, and guidance on SCRM are issued, in accordance with Executive Order 14028, the Bureau will have several opportunities to mature its SCRM program. Specifically, we noted the Bureau has not yet

- developed an organizationwide SCRM strategy that covers areas such as supply chain risk appetite and tolerance and acceptable supply chain risk mitigation strategies and controls, as outlined in NIST SP 800-53, Rev. 5[17]
- tailored the SCRM-related system security control requirements from NIST SP 800-53, Rev. 5, to its operational environment
- developed standard contract language requiring the identification of subcontractors used or verification that subcontractors are held to Bureau standards and several FedRAMP security clauses

Bureau officials noted that they will monitor the new governmentwide policies, standards, and guidance issued for SCRM and adjust the agency's processes accordingly. We will continue to monitor the Bureau's activities to mature its SCRM program as part of our future FISMA audits.

Protect

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

[17] We realize that an organization-level SCRM strategy that addresses risk appetite and tolerance will need to be integrated with the agency's ERM strategy. As noted in our recommendation follow-up section in appendix B, the Bureau is still in the process of establishing and implementing its ERM program, because it has not yet finalized its risk tolerance levels.

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

Security domains	Examples of components assessed by IGs
Configuration management	Configuration management plans, configuration settings, flaw remediation, and change control
Identity and access management	Identity, credential, and access management strategy; access agreements; least privilege; and separation of duties
Data protection and privacy	Security controls for exfiltration, data breach response plan, and privacy security controls
Security training	Assessment of skills, knowledge, and abilities; security awareness; and specialized security training

Source: U.S. Department of Homeland Security, *FY 2021 IG FISMA Reporting Metrics*.

Configuration Management

FISMA requires agencies to develop and implement 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.

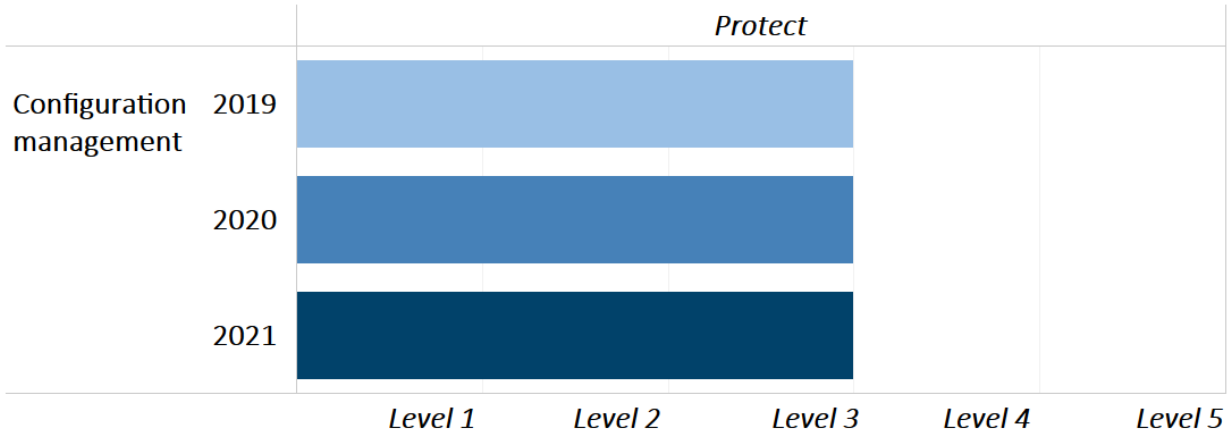
Current Agency Maturity

As in 2020, we found that the Bureau's configuration management program is operating at a level-3 (*consistently implemented*) maturity (figure 4), with the agency continuing to improve and perform some activities indicative of a higher maturity level. Specifically, we noted that the Bureau

- employs automated mechanisms to detect unauthorized hardware, software, and firmware as well as unauthorized changes to these components
- has consistently implemented a new mobile device management platform that can automate patch management and enforce Bureau mobile device operating system versions
- has implemented a vulnerability disclosure policy, in accordance with DHS's Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy*[18]

[18] U.S. Department of Homeland Security, *Develop and Publish a Vulnerability Disclosure Policy*, DHS Binding Operational Directive 20-01, September 2, 2020.

Figure 4. Maturity of the Configuration Management Domain, 2019–2021



Source: OIG analysis.

In addition, we have three recommendations from our previous FISMA audit reports that remain open related to strengthening the Bureau's configuration management program. These recommendations are related to strengthening vulnerability management practices, ensuring timely remediation of configuration-related vulnerabilities, and enforcing separation of duties in the agency's change control processes. The status of these recommendations is detailed in appendix B.

Opportunities for Improvement

While the Bureau's configuration management program is operating at a level-3 (*consistently implemented*) maturity, we identified an opportunity for improvement related to ensuring that the Bureau's configuration management plan is updated to reflect new technologies and processes.

Configuration Management Plan

As noted in NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*,[19] a configuration management plan provides a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. Specifically, this plan establishes a change control board, a methodology for selecting and naming configuration items that need to be placed under configuration management, and processes for monitoring and managing updates to baseline configurations. We found that the Bureau's configuration management plan was last updated in 2016 and does not reflect key changes in the agency's related processes and technologies. We believe that a key cause for this issue is competing organizational priorities as well as a focus on implementing a new technology that supports multiple organizational processes, in addition to configuration management.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires agencies to update their current configuration management policy and

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

associated procedures within an organization-defined frequency,[20] which the Bureau has determined to be whenever there is a significant change or every 5 years for policy and annually for procedures. Bureau officials informed us that they are planning to update the agency's configuration management plan by the end of 2021. Ensuring that the Bureau's configuration management plan is updated and maintained would provide the agency with additional assurance that configuration management roles and responsibilities are carried out effectively. We also believe that an updated configuration management plan will provide for greater continuity for new employees and contractors performing configuration management processes.

Recommendation

We recommend that the CIO

3. Ensure that the Bureau's configuration management plan is updated to reflect current processes, procedures, and technologies.

Management Response

The CIO concurs with our recommendation. In his response, the CIO states that the Bureau is currently updating its Configuration Management Plan to reflect current processes, procedures, and technologies. The Bureau's Configuration Management Plan is scheduled to be updated in the first quarter of fiscal year 2022.

OIG Comment

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

Identity and Access Management

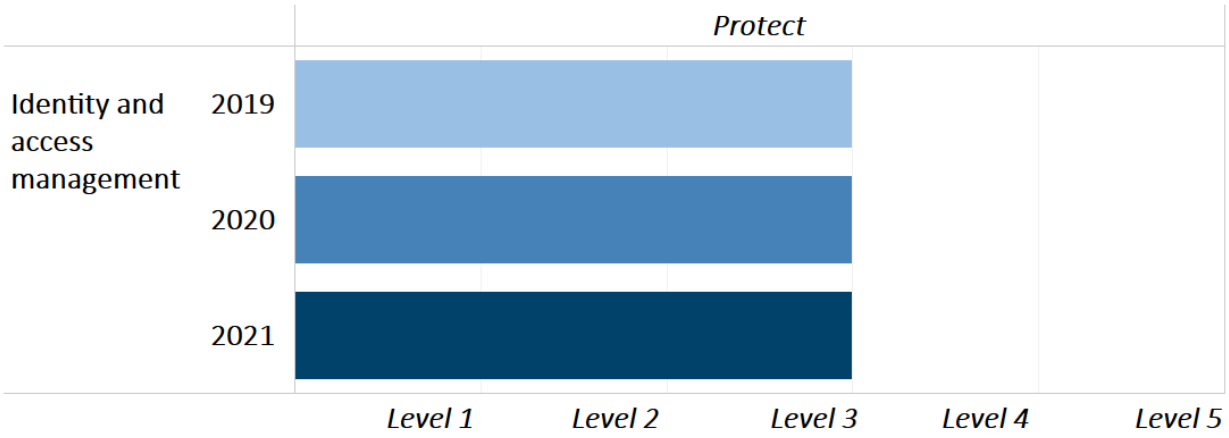
Identity and access management includes implementing a set of capabilities to ensure that users authenticate to IT resources and have access to only those resources that are required for their job function, a concept referred to as *need to know*. Supporting activities include onboarding and personnel screening, issuing and maintaining user credentials, and managing logical and physical access privileges, which are collectively referred to as *identity, credential, and access management* (ICAM).

Current Agency Maturity

As in 2020, we found that the Bureau's identity and access management program is operating at a level-3 (*consistently implemented*) maturity (figure 5).

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

Figure 5. Maturity of the Identity and Access Management Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Bureau continues to take steps to mature its ICAM program. Specifically, we noted the following:

- The Bureau has developed and implemented policies and procedures that cover multiple functions throughout the life cycle of a user's digital identity.
- The Bureau has developed an ICAM road map with implementation planned for 2023. The road map includes tasks supporting the redesign of privileged user access provisioning; further integration with the Bureau's single sign-on solution; and the incorporation of monitoring, reporting, and automation capabilities.

Opportunities for Improvement

Three recommendations from our previous FISMA audit reports remain open related to maturing the Bureau's identity and access management program. These recommendations concern implementing multifactor authentication and strengthening access management processes for privileged and nonprivileged users. The status of these recommendations is detailed in appendix B. We will continue to monitor the Bureau's progress in maturing its identity and access management program as part of our future FISMA audits.

Data Protection and Privacy

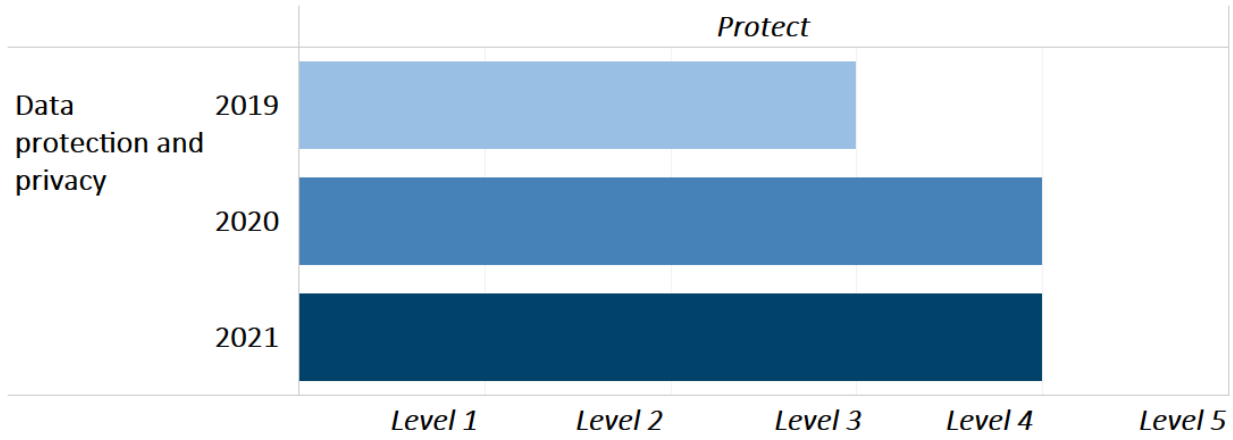
Data protection and privacy refers to a collection of activities focused on preserving authorized restrictions on information access and protecting personal privacy and proprietary information. Effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their personally identifiable information increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, federal guidance requires covered federal agencies to develop, implement, and maintain agencywide privacy programs that, where personally identifiable information is

involved, play a key role in information security and implementing the NIST Risk Management Framework.[21]

Current Agency Maturity

As in 2020, we found that the Bureau's data protection and privacy program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 6).

Figure 6. Maturity of the Data Protection and Privacy Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Bureau has strengthened its data protection and privacy processes related to planning and breach response. Specifically, we noted that the Bureau

- updated its privacy program plan
- continues to conduct privacy training for personnel
- refined its data breach response processes based on lessons learned

We have one recommendation from our 2019 FISMA audit that remains open related to the deployment of technology used by the Bureau to monitor and control data exfiltration. The status of this recommendation is detailed in appendix B.

Opportunities for Improvement

This year, we identified an additional opportunity for improvement related to the consistency of information contained in some of the Bureau's privacy incident tickets. Bureau officials indicated that staff turnover led to tickets being filled out without all required data and that they have since resolved this resource issue. Further, officials stated that the tool being used to maintain the privacy incident tickets will be updated to enforce the completion of all required fields for a ticket before closure. Based on these actions, we are not making a recommendation in this area, and we will continue to monitor the Bureau's progress in this area as part of future FISMA audits.

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

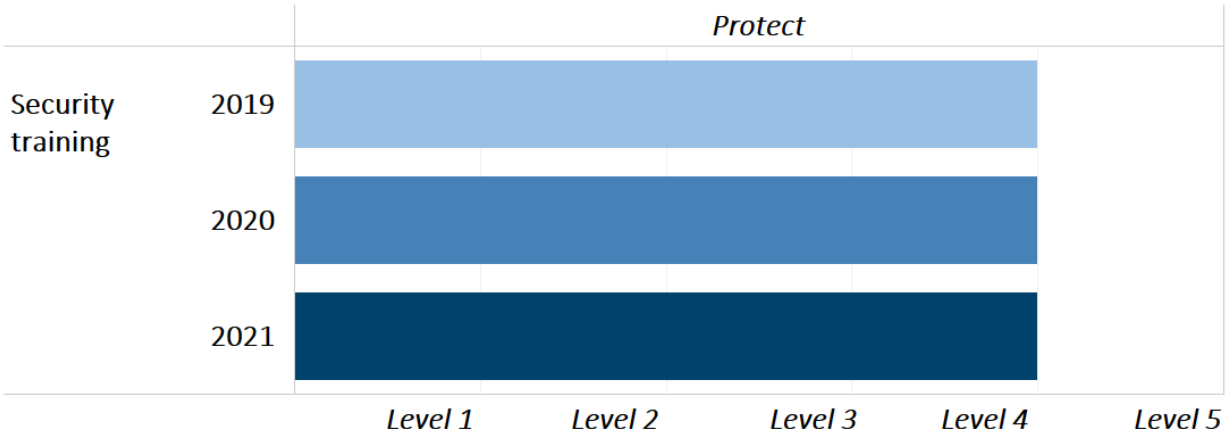
Security Training

FISMA requires agencies to develop an information security program that provides security awareness training to personnel, including contractors, who support the operations and assets of the organization, as well as role-based training for individuals with significant information security responsibilities. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, notes that in general, people are one of the weakest links in attempting to secure agency systems and networks.[22] As such, a robust, enterprisewide security awareness and training program is paramount to ensuring that people understand their IT security responsibilities and organizational policies and know how to properly use and protect the IT resources entrusted to them.

Current Agency Maturity

As in 2020, we found that the Bureau's security training program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 7).

Figure 7. Maturity of the Security Training Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Bureau has continued to maintain effective information security processes in the areas of cybersecurity workforce assessment, phishing exercises, and security awareness training. Specifically, we noted that the Bureau

- completed a knowledge, skills, and abilities survey assessment of its employees and is planning to use the results to update its security training curriculum
- updated its phishing exercises to include simulations based on employee work roles
- is using user feedback as an input to update the agency's security training program on a near-real-time basis

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

Opportunities for Improvement

While the Bureau's security training program is operating effectively at level 4 (*managed and measurable*), we noted that the Bureau can update its policies and procedures on a timelier basis and use the outputs from the agency's information security continuous monitoring (ISCM) and developing ERM programs to inform updates to its security awareness and training program. We will continue to monitor the Bureau's progress in this area as part of our future FISMA audits.

Detect

The objective of the *detect* function in NIST's Cybersecurity Framework is to implement activities to discover and identify the occurrence of cybersecurity events in a timely manner. The Cybersecurity Framework notes that continuous monitoring processes are used to detect anomalies and changes in the organization's operational environment, maintain knowledge of threats, and ensure security control effectiveness. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2021 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

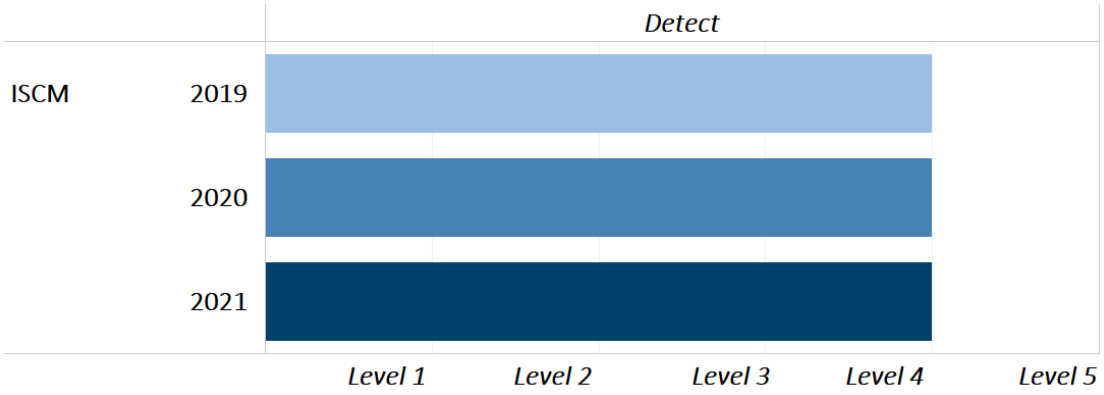
ISCM refers to the process of maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Best practices for implementing ISCM are outlined in NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*.[23] This publication notes that a key component of an effective ISCM program is a comprehensive ISCM strategy based on a risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission and business impacts.

Current Agency Maturity

As in 2020, we found that the Bureau's ISCM program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 8).

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

Figure 8. Maturity of the ISCM Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Bureau has continued to effectively implement its ISCM program. Specifically, we noted the Bureau

- updated its *Information Security Continuous Monitoring Process* standard operating procedure in September 2021 to reflect the new August 2020 *Risk Management Handbook*, which provides guidance for monitoring controls, analyzing ISCM data, and reporting findings
- completed the 3-year-cycle ISCM assessments
- created an ISCM annual report that includes the Bureau's progress on performing various aspects of continuous monitoring, such as ongoing assessments, ongoing authorizations, and malware detection

Opportunities for Improvement

Our 2017 and 2019 FISMA audit reports include recommendations that remain open related to ensuring that security assessment and authorization processes are performed before deploying systems and establishing risk tolerance levels. We believe that addressing these recommendations could help the Bureau mature its ISCM program. The status of these recommendations is detailed in appendix B.

Respond

The objective of the *respond* function in NIST's Cybersecurity Framework is to implement processes to contain the impact of detected cybersecurity events. Activities include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*, that we assessed include the Bureau's incident detection, analysis, handling, and reporting processes.

Incident Response

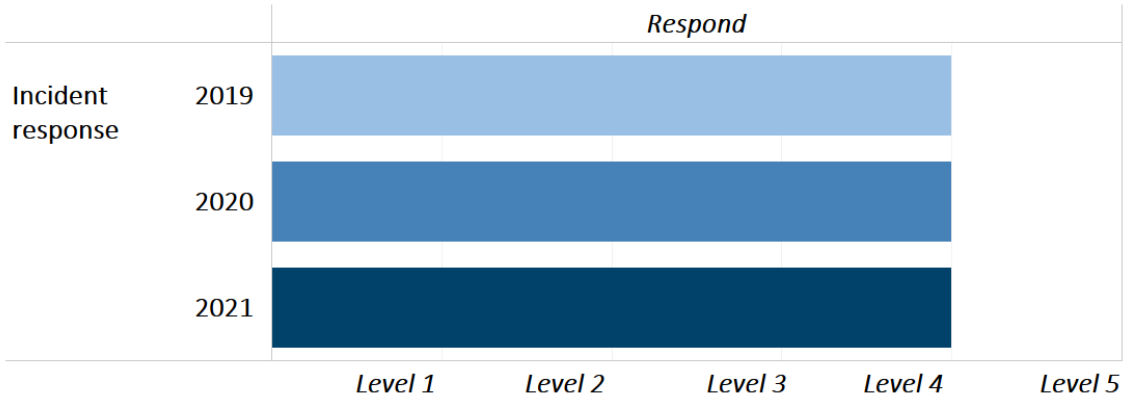
FISMA requires each agency to develop, document, and implement an agencywide information security program that includes policies and procedures for incident response. Best practices for incident response

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 key phases: preparation; detection and analysis; containment, eradication, and recovery; and postincident activity.[24]

Current Agency Maturity

As in 2020, we found that the Bureau's incident response program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 9).

Figure 9. Maturity of the Incident Response Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Bureau has continued to mature information security processes in the areas of cybersecurity incident ticketing, quantitative and qualitative performance metrics, and malware detection. Specifically, we noted the Bureau

- has implemented a new incident ticketing system that is more closely integrated with configuration management activities
- continues to capture and assess incident response performance measures, including for reporting to the United States Computer Emergency Readiness Team
- has begun using a new program that identifies artifacts and systems that may have an association with malware

Opportunities for Improvement

The Bureau is in the process of strengthening its technologies for data loss protection and advanced incident response to assist in behavioral baselining. Further, our 2019 FISMA audit report includes a recommendation that remains open related to the deployment and coverage of the Bureau's data loss protection tool that we believe will impact the maturity of the incident response program. The status of this recommendation is detailed in appendix B.

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

Recover

The objective of the *recover* function in NIST's Cybersecurity Framework is to ensure that organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The Cybersecurity Framework outlines contingency planning processes that support timely recovery to normal operations and reduce the impact of a cybersecurity event. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*, that we assessed include the Bureau's processes for developing and testing information system contingency plans and the management of contingency planning considerations related to the agency's information and communications technology supply chain.

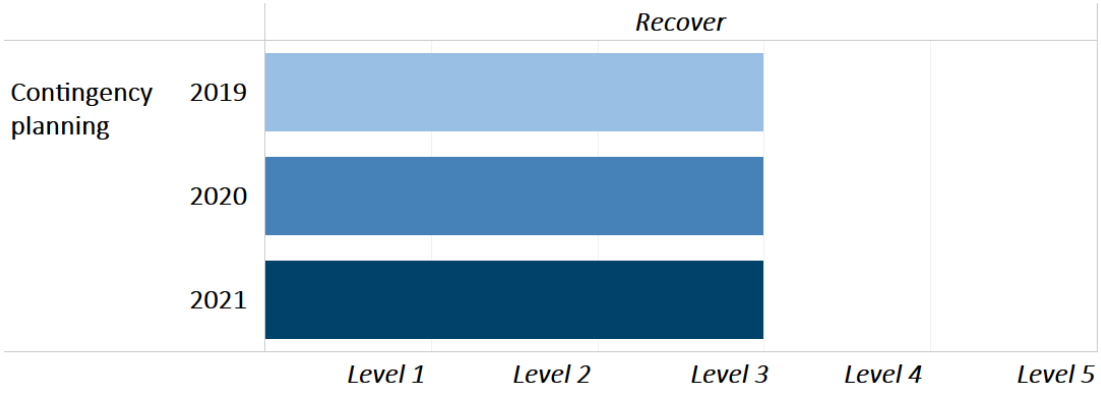
Contingency Planning

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*, provides best practices for information system contingency planning.[25]

Current Agency Maturity

As in 2020, we found that the Bureau's contingency planning program operates at a level-3 (*consistently implemented*) maturity (figure 10).

Figure 10. Maturity of the Contingency Planning Domain, 2019–2021



Source: OIG analysis.

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

This year, we found that the Bureau has continued to consistently implement information security processes in the areas of roles and responsibilities, backup and storage processes, and policies and procedures. Specifically, we noted that the Bureau

- has documented its roles and responsibilities for contingency in its Continuity of Operations Plan
- continues to document its backup and storage processes
- has updated its Information Technology Contingency Plan to reflect its current system inventory

Opportunities for Improvement

Bureau officials notified us that additional resources are needed to further mature the contingency planning program. Further, we believe that the agency should continue to monitor and incorporate into its contingency planning program, as appropriate, information and communications technology supply chain guidance. We will continue to monitor the Bureau's efforts to mature its contingency planning program as part of our future FISMA audits.

Appendix A: Scope and Methodology

Our specific audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. To accomplish our objectives, we reviewed the effectiveness of the Bureau's information security program across the five function areas outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*: *identify*, *protect*, *detect*, *respond*, and *recover*. These five function areas consist of nine security domains: risk management, SCRM, configuration management, identity and access management, data protection and privacy, security training, ISCM, incident response, and contingency planning.

To assess the effectiveness of the Bureau's information security program, we

- analyzed security policies, procedures, and documentation
- interviewed Bureau management, staff, and contractors
- performed vulnerability scanning at the network, operating system, and database levels for select systems[26]
- observed and tested specific security processes and controls at the program level
- engaged with a contractor to assess select controls for two information systems[27]
- performed data analytics using a commercially available tool to support our effectiveness conclusions for multiple areas

We contracted with an independent public accounting firm who assessed the effectiveness of the Bureau's identity and access management and data protection and privacy domains. We reviewed and monitored the work of the contractor to ensure compliance with the contract and *Government Auditing Standards*.

To rate the maturity of the Bureau's information security program and functional areas, we used the scoring methodology defined in DHS's *FY 2021 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 June 2021 to September 2021. 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.

[26] We plan to transmit the detailed results of our vulnerability scanning to the Bureau in a separate, restricted memorandum because of the sensitive nature of the information.

[27] We plan to transmit the detailed results of our testing of these systems under a separate, restricted memorandum because of the sensitive nature of the information. We provided oversight of the contractor throughout the system assessments to ensure that they met auditing standards.

Appendix B: Status of Prior FISMA Recommendations

As part of our 2021 FISMA audit, we reviewed the actions taken by the Bureau to address the outstanding recommendations from our previous FISMA audit reports. Below is a summary of the status of the 11 recommendations that were open at the start of our 2021 FISMA audit (table B-1). Based on corrective actions taken by the Bureau, we are closing 2 recommendations related to mobile device configuration management and completion of system-level BIAs. The remaining 9 recommendations—which are related to risk management, configuration management, data protection and privacy, and identity and access management—remain open. We will update the status of these recommendations in our spring 2022 semiannual report to Congress, and we will continue to monitor the Bureau's progress in addressing our open recommendations as part of our future FISMA audits.

Table B-1. Status of 2014–2020 FISMA Recommendations That Were Open as of the Start of Our Fieldwork, by Security Domain

Year		Recommendation	Status	Explanation
Risk management				
2017	1	We recommend that the chief risk officer continue to work with divisions across the Bureau to ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.	Open	Although the Bureau continues to make progress in establishing and implementing its ERM program, including defining a risk appetite statement, it has not yet finalized its risk tolerance levels. Bureau officials informed us that the agency plans to define risk tolerance levels once a new director has been appointed.
2019	2	We recommend that the CIO ensure that established security assessment and authorization (SA&A) processes are performed prior to the deployment of all cloud systems used by the Bureau.	Open	We continue to identify instances in which the Bureau has placed systems into production prior to completing its SA&A processes.

Year		Recommendation	Status	Explanation
Configuration management				
2014	3	We recommend that the CIO strengthen the Bureau's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.	Open	The Bureau has implemented an automated solution for assessing application-level security configurations for web applications but has not done so for assessing and managing database security configurations. According to Bureau officials, the agency has purchased a database scanning technology and plans to implement it by the end of 2021.
2018	1	We recommend that the CIO strengthen configuration management processes by (a) remediating configuration-related vulnerabilities in a timely manner and (b) ensuring that optimal resources are allocated to perform vulnerability remediation activities.	Open	The Bureau has implemented process and technological changes that have significantly reduced the number of critical and high-risk vulnerabilities that remain open past the required remediation dates. However, we continue to identify, as does the Bureau's internal vulnerability scanning, that the agency is not remediating numerous critical or high-risk vulnerabilities in a timely manner.
2018	2	We recommend that the CIO develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.	Closed	This year, we found that the Bureau implemented a new mobile device management system, created standard operating procedures, and implemented mitigating controls for agency-issued mobile phones that have not been updated to approved patch levels. Further, we verified the timely application of patches for agency-issued mobile phones.
2020	1	We recommend that the CIO ensure that (a) change control policies and procedures address separation of duties in the change management life cycle and (b) separation of duties is enforced in the Bureau's change control tool.	Open	The Bureau plans to implement a technical change to restrict the individuals allowed to close tickets in the agency's change control tool. Further, our testing of change control tickets this year continued to identify inadequate separation of duties.

Year	Recommendation		Status	Explanation
Identity and access management				
2017	2	We recommend that the CIO develop and implement a tiered approach for implementing multifactor authentication that considers system risk levels and user roles and uses lessons learned to inform broader adoption.	Open	The Bureau has enabled personal identity verification usage for both privileged and nonprivileged users. The agency has also begun enforcing the use of personal identity verification for privileged users and is finalizing its plans to do so for nonprivileged users.
2018	3	We recommend that the CIO determine whether established processes and procedures for management of user-access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.	Open	Bureau officials informed us that the agency has begun a project to implement a solution to effectively manage user access agreements and rules of behavior for privileged users.
2019	3	We recommend that the CIO ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonprivileged users.	Open	Bureau officials informed us that the agency has begun a project to implement a solution to effectively manage user access agreements and rules of behavior for nonprivileged users.
Data protection and privacy				
2019	5	We recommend that the CIO perform a risk assessment to determine (a) the optimal deployment of the Bureau's technology for monitoring and controlling data exfiltration to all network access points and (b) appropriate access to internet storage sites.	Open	The Bureau has completed an assessment of the deployment of technology for monitoring and data exfiltration and has identified a tool that may be used. The Bureau has accepted this risk while it pursues this tool, and we will assess the agency's implementation of the tool once it is finalized.
Contingency planning				
2019	7	We recommend that the CIO ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.	Closed	The Bureau has completed system-level BIAs for 21 of 22 systems on its FISMA inventory and has scheduled the final system-level BIA to be completed.

Source: OIG analysis.

Appendix C: Management Response

1700 G Street NW, Washington, D.C. 20552

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

October 26, 2021

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

Dear Associate Inspector General Sheridan,

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the *2021 Audit of the Bureau's Information Security Program*. We are pleased that you found the Bureau's information security program is operating at an overall level 4 (*managed and measurable*) maturity based on the OIG's Federal Information Security Modernization Act of 2014 (FISMA) maturity model. In Fiscal Year (FY) 2022, the Bureau will continue to enhance its processes and technologies to raise its overall maturity to level 5 (*optimized*) 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 3 maturity (*consistently implemented*) for the **Identify** function.

- The Bureau's Risk Management program is operating at level 3 maturity (*consistently implemented*). This year, the Bureau updated its risk management policies and procedures, developed a risk appetite statement, used a tool to support centralized hardware asset management, and maintained qualitative and quantitative performance measures related to its plans of action and milestones (POA&M) process. In FY2022, the Bureau will continue to improve its enterprise and cybersecurity risk management programs by finalizing enterprise risk tolerances and work to implement processes that will prohibit future instances of information systems being placed into production without

consumerfinance.gov

completion of Security Assessment & Authorization (SA&A) activities. Additionally, the Bureau will work to address recommendations pertaining to identifying security and privacy risks through the cybersecurity risk register process and ensuring all appropriate system-level vulnerabilities are managed.

- Supply Chain Risk Management (SCRM) is a new domain and the Bureau will not be rated this year. The Bureau will leverage government-wide policies, standards, and guidance, in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity,* to mature. This year, the Bureau finalized its Cybersecurity Supply Chain Risk Management (C-SCRM) Process. This document includes processes used by the Bureau's Office of Cybersecurity to manage cybersecurity-related supply chain risks. In FY2022, CFPB will mature C-SCRM processes by tailoring SCRM related system security control requirements issued the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* to its operational environment and developing standard contract language that holds contractors and subcontractors to Bureau standards and Federal Risk and Authorization Management Program (FedRAMP) security clauses.

The Bureau is operating at a level 4 maturity (*managed and measurable*) for the **Protect** function.

- The Bureau's Configuration Management program is operating at level 3 maturity (*consistently implemented*). This year, the CFPB employed automated mechanisms to detect unauthorized hardware, software, and firmware as well as unauthorized changes to these components. The Bureau also implemented a vulnerability disclosure policy, in accordance with Department of Homeland Security (DHS) Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy*. Lastly, the Bureau implemented a new mobile device management platform that provided automated patch management and enforcement capabilities, which closed a recommendation from 2018. In FY2022, the Bureau will continue to address open recommendations related to strengthening vulnerability management practices, ensuring timely remediation of configuration-related vulnerabilities, and ensure separation of duties are enforced through change control processes. Additionally, CFPB will ensure its configuration management plan is updated and maintained.

- The Bureau's Identity and Access Management (ICAM) program is operating at level 3 maturity *(consistently implemented).* This year, CFPB implemented account management, audit logging, and background investigation policies and procedures used to manage digital identities. Additionally, CFPB developed an ICAM roadmap with full

implementation planned for FY2022. The roadmap includes tasks supporting the redesign of privileged user access provisioning, further integration with the Bureau's single-sign-on solution, and the incorporation of monitoring and reporting processes. In FY2022, per open recommendations, the Bureau plans to improve its identity and access management program by implementing tools that will enforce multifactor authentication (MFA) for privileged and non-privileged users. In addition, a new configuration management tool will automate privileged access management for user-access agreements and rules-of-behavior policies.

- The Bureau's Data Protection and Privacy program is operating at level 4 maturity (*managed and measurable)*. This year, CFPB updated its privacy program plan, continued to conduct privacy training for all required personnel, and refined its data breach response processes based on lessons learned. In FY2022, CFPB will continue to improve the accuracy and consistency of the information contained in the Bureau's privacy incident tickets. Additionally, the Bureau will continue strengthening its technologies to monitor and control data exfiltration across the enterprise.

- The Bureau's Security Training program is operating at level 4 maturity (*managed and measurable)*. This year, the CFPB improved its security training program by completing a knowledge, skills, and abilities survey assessment of its employees and used the results to update its security training curriculum. Additionally, the Bureau updated its phishing exercises to include simulations based on employee work roles and utilized user feedback as an input to update the agency's security training on a near real-time basis. In FY2022, the BFCP plans to use the outputs from Enterprise Risk Management and Information Security Continuous Monitoring (ISCM) programs to update its security awareness and training program.

The Bureau is operating at a level 4 maturity *(managed and measurable)* for the **Detect** function.

- CFPB's ISCM program continues to operate at level 4 maturity *(managed and measurable)*. The Bureau has updated its ISCM process document to reflect updated risk management policy and procedures, identified ISCM staff skill gaps and training needs, and completed 3-year cycle assessments and produced a 3-year trend analysis report. In addition, the Bureau created an ISCM annual report that includes progress on performing various aspects of continuous monitoring such as ongoing assessments and authorizations and malware detection. In FY2022, the Bureau will improve its ISCM program by ensuring SA&A processes are performed prior to the deployment of information systems and the establishment of risk tolerance levels.

The Bureau is operating at a level 4 maturity *(managed and measurable)* for the **Respond** function.

- The Bureau's Incident Response program continues to operate at level 4 maturity (*managed and measurable*). CFPB implemented a new incident ticketing system that provides closer integration with configuration management activities. The Bureau continued to capture and assess incident response performance measures, including reporting to the United States Computer Emergency Readiness Team (US-CERT). Additionally, the Bureau began using a new program to identify artifacts and systems potentially associated with malware to automatically inform users. In FY2022, the Bureau will continue to strengthen its technologies for data loss protection and advanced incident response to assist in behavior baselining.

The Bureau is operating at a level 3 maturity (*consistently implemented)* for its **Recover** function.

- The Bureau's Contingency Planning program is operating at a level 3 maturity (*consistently implemented*). CFPB has documented its roles and responsibilities for contingency in the Bureau's Continuity of Operations Plan, continued to implement backup and storage processes in accordance with CFPB policies and procedures, and updated its Information Technology Contingency Plan (ITCP) to reflect the current system inventory. Lastly, the Bureau closed a recommendation from 2019 by developing system-level Business Impact Analyses (BIAs) and incorporating the results into contingency planning strategies and processes. In FY2022, CFPB will continue to monitor and incorporate information and telecommunications technology (ICT) supply chain guidance into its contingency planning program.

We appreciate the OIG for noting CFPB'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,

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2021.10.26 13:29:16 -04'00'

Chris Chilbert
Chief Information Officer

Response to recommendations presented in the OIG Draft Report: *2021 Audit of the Bureau's Information Security Program*

Recommendation 1: Develop and implement a cyber risk register process to aggregate information system, business process and enterprise level risks.

Management Response:

The Bureau concurs with the auditor's recommendation. In FY2021, the Office of Technology & Innovation (T&I) implemented a risk management program. This program established risk profiles for T&I, which included a cybersecurity risk profile, to document major information technology risks. The Bureau's Office of Cybersecurity will leverage the existing cybersecurity risk register to coordinate with the Bureau and T&I's risk management programs to implement an escalation process that aggregates information systems, business processes, and enterprise-level risks.

Recommendation 2: Strengthen oversight processes to ensure the creation of POA&M items for weaknesses identified through vulnerability scanning activities.

Management Response:

The Bureau concurs with the auditor's recommendation. The Bureau's Office of Cybersecurity is responsible for POA&M management. As such, the Office of Cybersecurity is updating POA&M processes to create POA&M items for weaknesses identified through vulnerability scanning activities in accordance with vulnerability criticality and remediation thresholds. This activity scheduled to be updated by Fy2022 Q4.

Recommendation 3: Ensure that the Bureau's configuration management plan is updated to reflect current processes, procedures, and technologies

Management Response:

The Bureau concurs with the auditor's recommendation. The Bureau is currently updating its Configuration Management Plan to reflect current processes, procedures, and technologies. The Bureau's Configuration Management Plan is scheduled to be updated in FY2022 Q1.

Abbreviations

BIA	business impact analysis
CIO	chief information officer
DHS	U.S. Department of Homeland Security
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
ICAM	identity, credential, and access management
IG	inspector general
ISCM	information security continuous monitoring
IT	information technology
NIST	National Institute of Standards and Technology
POA&M	plan of action and milestones
SA&A	security assessment and authorization
SCRM	supply chain risk management
SP 800-53, Rev. 5	Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
T&I	Office of Technology and Innovation

Report Contributors

Khalid Hasan, Senior OIG Manager for Information Technology
Andrew Gibson, OIG Manager, Information Technology Audits
Jeffrey Woodward, Senior Policy and Planning Analyst
Chelsea Nguyen, Senior IT Auditor
Justin Byun, IT Auditor
Trang Do, IT Auditor
Melissa Fortson, IT Auditor
Nick Gallegos, Criminal Investigator
Lauren Alston, IT Audit Intern
Justin Wu, IT Audit Intern
Alexander Karst, Senior Information Technology Management Specialist
Fay Tang, Senior Information Technology Management Specialist
Peter Sheridan, Associate Inspector General for Information Technology

Contact Information

General

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

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

Media and Congressional

OIG.Media@frb.gov

Hotline

Report fraud, waste, and abuse.

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

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

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