Evaluation Report
2019-IT-C-009
July 17, 2019

Bureau of Consumer Financial Protection

The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP

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-009, July 17, 2019

The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP

Findings

The Bureau of Consumer Financial Protection (Bureau) has developed a life cycle process for deploying and managing security risks for Bureau systems, which include the Federal Risk and Authorization Management Program (FedRAMP) cloud systems it uses. However, we found that the process is not yet effective in ensuring that (1) risks are comprehensively assessed prior to deploying new cloud systems, (2) continuous monitoring is performed to identify security control weaknesses after deployment, and (3) electronic media sanitization renders sensitive Bureau data unrecoverable when cloud systems are decommissioned.

Specifically, we found that the Bureau did not perform an agency-specific risk and security controls assessment and grant an authorization to operate for a FedRAMP cloud system supporting a key agency mission. We also found that the Bureau did not ensure that the FedRAMP Project Management Office had an accurate inventory of the cloud systems used by the agency. This inaccurate inventory hindered the Bureau's ability to perform effective continuous monitoring activities and resulted in weaknesses in verifying incident reporting and contingency plan testing processes for cloud service providers. During our fieldwork, the Bureau implemented an automated process to ensure that accurate inventory information was provided to the FedRAMP Project Management Office. We also found that the Bureau can obtain additional assurance that electronic media sanitization activities performed by cloud service providers render sensitive Bureau data unrecoverable.

Recommendations

This report includes three recommendations designed to strengthen the Bureau's life cycle processes for leveraging FedRAMP cloud systems in the areas of risk management, continuous monitoring, and electronic media sanitization. The Bureau concurs with our recommendations and outlined plans to implement them. We will continue to monitor the Bureau's progress in addressing these recommendations as part of future reviews.

Purpose

The Federal Information Security Modernization Act of 2014 requires that we perform an annual independent evaluation of the Bureau's information security program and practices, including testing the effectiveness of security controls for select information systems. Our objective was to determine whether the Bureau has implemented an effective life cycle process for deploying and managing FedRAMP cloud systems used by the agency, including ensuring that effective security controls are implemented.

Background

FedRAMP was established in 2011 to provide federal agencies with a cost-effective, risk-based approach for the adoption and use of cloud computing services. Since its establishment in July 2011, the Bureau has embraced cloud computing as a model to meet its information technology needs in a flexible, scalable manner. The Bureau uses five FedRAMP cloud systems to support various mission and business processes. As part of its technology vision, the Bureau plans to move to a cloud-only information technology infrastructure by 2022.

Recommendations, 2019-IT-C-009, July 17, 2019

The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP

Finding 1: The Bureau Should Consistently Use Security Assessment, Authorization, and Monitoring Processes to Manage Security Risks for Its FedRAMP Cloud Systems

Number	Recommendation	Responsible office
1	Ensure that established SA&A processes are a. performed prior to the deployment of all FedRAMP cloud systems used by the Bureau. b. used to make an agency-specific authorization decision for the system that is in production and noted in our report.	Office of Technology and Innovation
2	Ensure that a. continuous monitoring information provided by the PMO or the CSP, as appropriate, is obtained and reviewed in a timely manner for all FedRAMP cloud systems used by the Bureau. b. for any gaps identified, including for incident response and contingency testing, a risk assessment is performed to determine appropriate responses.	Office of Technology and Innovation

Finding 2: The Bureau Can Obtain Greater Assurance on the Effectiveness of Electronic Media Sanitization Performed by CSPs

Number	Recommendation	Responsible office
3	Evaluate and implement, as appropriate, options to obtain additional assurance that electronic media sanitization performed by CSPs renders sensitive Bureau data unrecoverable when assets are decommissioned.	Office of Technology and Innovation

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

MEMORANDUM

DATE: July 17, 2019

TO: Katherine Sickbert
Acting Chief Information Officer
Bureau of Consumer Financial Protection

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2019-IT-C-009: *The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP*

We have completed our report on the subject evaluation. We performed this evaluation pursuant to the Federal Information Security Modernization Act of 2014, which requires each agency Inspector General to conduct an annual independent evaluation of the effectiveness of the agency's information security program and practices, including testing controls for select systems. We conducted this evaluation to determine whether the Bureau of Consumer Financial Protection (Bureau) has implemented an effective life cycle process for deploying and managing its cloud systems, including ensuring that effective security controls are implemented.

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

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

cc: Tiina Rodrigue, Chief Information Security Officer
Kate Fulton, Chief Operating Officer
Marianne Roth, Chief Risk Officer
Kirsten Sutton, Chief of Staff
Elizabeth Reilly, Chief Financial Officer
Dana James, Deputy Chief Financial Officer
Lauren Hassouni, Finance and Policy Analyst
Carlos Villa, Finance and Policy Analyst

Contents

Introduction

Objective

Our overall objective is to determine whether the Bureau of Consumer Financial Protection (Bureau) has implemented an effective life cycle process for deploying and managing cloud systems that have been approved for federal agency use through the Federal Risk and Authorization Management Program (FedRAMP). In addition, our objective includes determining whether the Bureau has implemented effective security controls for the FedRAMP cloud systems it uses.[1] The first phase of this evaluation, which is the subject of this report, focused on determining the effectiveness of the Bureau's life cycle and risk management processes for deploying and managing FedRAMP cloud systems. As part of phase 2, we plan to determine the effectiveness of the security controls implemented by the Bureau for select FedRAMP cloud systems. Our scope and methodology are detailed in appendix A.

Background

In December 2010, as part of the federal government's information technology (IT) modernization effort, the Office of Management and Budget adopted the *Cloud First Policy*.[2] This policy was intended to accelerate the pace at which the federal government would realize the value of cloud computing[3] by requiring agencies to evaluate safe, secure cloud computing options before making new investments. To support federal agencies' adoption of secure cloud computing solutions, FedRAMP was established in December 2011.[4] One of the goals of FedRAMP is to provide a cost-effective, risk-based approach for the adoption and use of cloud services by federal agencies through standardizing security requirements, establishing an independent security assessment program for cloud service providers (CSPs), and making available security authorization packages and related documentation. Federal agencies can use FedRAMP to speed the adoption of cloud systems through the reuse of security assessments and related documentation by a do once, use many times approach.

Figure 1 highlights the key stakeholders involved in FedRAMP.

- The FedRAMP Project Management Office (PMO), housed at the U.S. General Services Administration, serves as the overall facilitator of and liaison for FedRAMP processes. In this capacity, the PMO is responsible for establishing unified documentation and processes, offering

[1] The Bureau has deployed cloud systems that are not offered through FedRAMP; those systems are not included in our scope.

[2] Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management*, December 9, 2010. In September 2018, the Office of Management and Budget updated its *Federal Cloud Computing Strategy* to provide additional guidance for cloud security, procurement, and workforce management.

[3] *Cloud computing* refers to a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing technology can include hosted email solutions provided by a private company or a scalable application running on a government-owned data center.

[4] Office of Management and Budget Memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011.

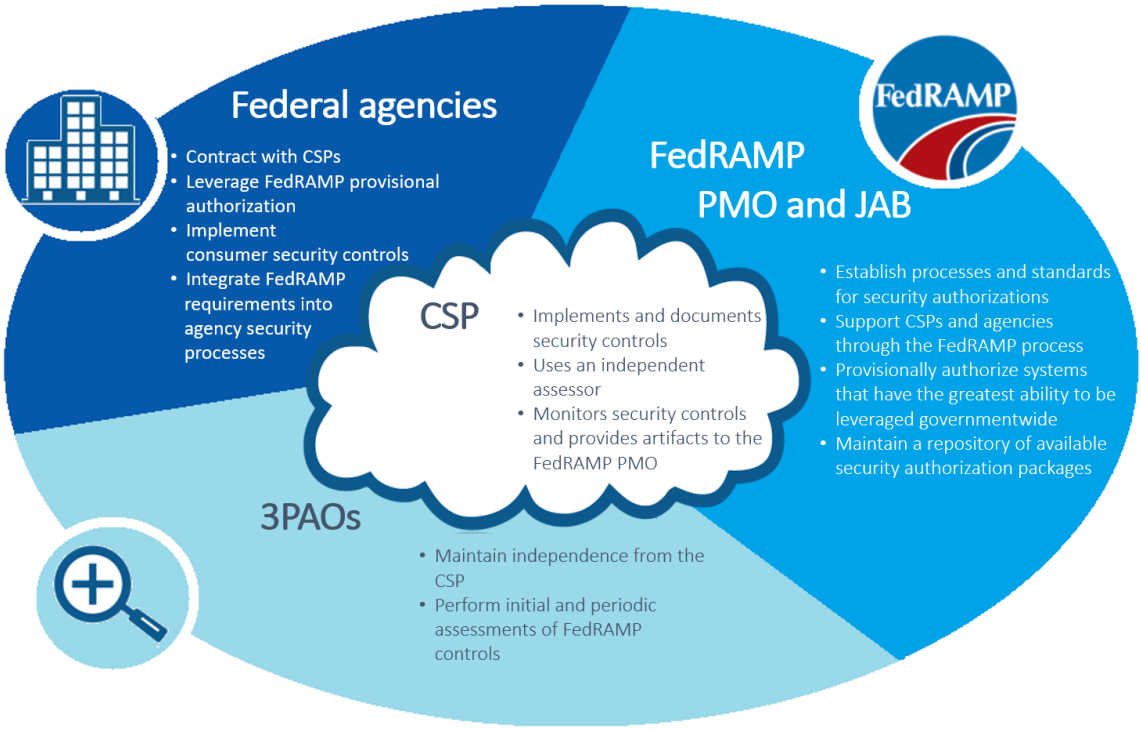
guidance, maintaining a secure repository of the authorization to operate (ATO) packages, prioritizing requests for authorizations, and managing a continuous monitoring and incident response and reporting framework. The PMO also provides project management support to the Joint Authorization Board (JAB).

- The JAB, which consists of members from the U.S. Department of Defense, the U.S. Department of Homeland Security, and the U.S. General Services Administration, reviews and provides provisional security authorizations of cloud solutions. The JAB's responsibilities include approving accreditation criteria for third-party assessment organizations (3PAOs).

- The 3PAOs provide overall discovery, testing, and validation of CSP offerings and present findings to the PMO and the JAB. The 3PAOs also perform updated testing based on gaps identified in CSP offerings.

- Federal agencies are responsible for reviewing the CSP's authorization package and determining whether the level of risk associated with the system is acceptable. Agencies are required to issue their own ATO to formally accept the risk of using the FedRAMP cloud system and to provide ATO documentation to the PMO.

Figure 1. Key FedRAMP Stakeholders



Source. OIG analysis of June 2014 FedRAMP Industry Day presentation and various PMO documents.

The Bureau's Use of FedRAMP Cloud Systems

Since its establishment in July 2011, the Bureau has embraced cloud computing as a model to meet its IT needs in a flexible, scalable manner. In April 2018, the Bureau developed its *2022 Target Architecture Plan*. The plan outlines the Bureau's technological vision for a complete migration to a cloud-only infrastructure by 2022. The plan states that some of the benefits of moving to a cloud-only infrastructure include reducing costs, gaining access to the most up-to-date technology, and improving quality of service.

The Bureau is leveraging five FedRAMP cloud systems to support the agency's mission and business processes (table 1).

Table 1. FedRAMP Cloud Systems Used by the Bureau

CSP	Cloud system used	Cloud type and description
Amazon/Akamai	Amazon Web Services	A multitenant public cloud[a] offering that operates under an infrastructure-as-a service model. Through this offering, agencies can access on-demand computing resources, such as servers, storage, network infrastructure, and various other web services.
	Content Delivery Services	A public cloud offering that operates under an infrastructure-as-a-service model. Through this offering, agencies can use a platform to improve the performance and customer experience of web content.
General Dynamics Information Technology	Customer eXperience Platform	A government community cloud that operates under a platform-as-a-service model. Through this offering, agencies can deploy scalable and tailorable contact center operations.
Salesforce	Salesforce Government Cloud	A government community cloud that operates under a platform-as-a-service and software-as-a-service model. Through this offering, agencies can deploy systems and leverage various services such as sales, communities, and industry solutions.
Cylance	CylancePROTECT	A private cloud that operates under a software-as-a-service model. Through this offering, agencies can detect and prevent malware from executing on endpoints in real time.

Source. OIG analysis of information available on the FedRAMP Marketplace.

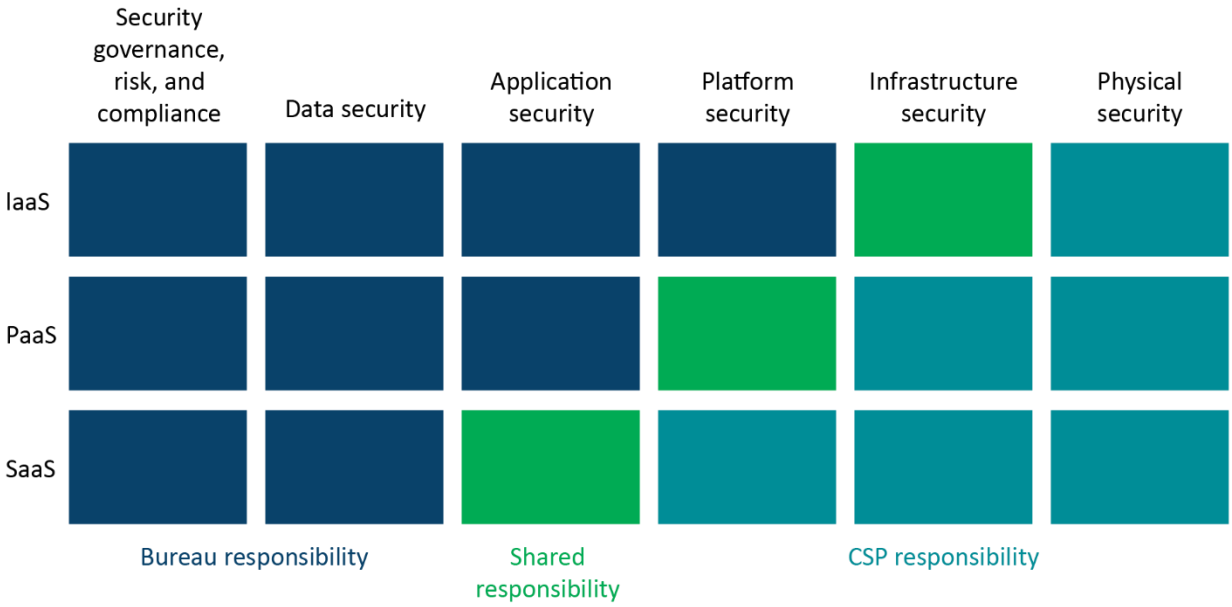
[a] A multitenant cloud allows customers to share computing resources in a public or private cloud architecture. Each tenant's data are isolated and remain invisible to other tenants. In a public cloud, the customers are often different organizations. This model allows the CSP to run one server instance, which is less expensive and makes it easier to deploy updates to a large number of customers.

The Bureau's use of FedRAMP cloud systems spans infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) models.

- The IaaS is a cloud computing model in which the consumer can provision processing, storage, networks, and other computing resources and deploy and run arbitrary software.
- The PaaS cloud computing model provides the capability to deploy onto the cloud infrastructure consumer-created or consumer-acquired applications using programming languages and tools supported by the provider.
- The SaaS cloud computing model provides the capability to use the provider's applications running on a cloud infrastructure.

Primary security responsibilities for the Bureau vary depending on the type of cloud computing model used (figure 2). However, the Bureau retains primary responsibility for security governance, risk, compliance, and data security, irrespective of the cloud model chosen.

Figure 2. Cloud Responsibility Matrix by Cloud Service Model



Source. OIG analysis of information presented in *The Official (ISC)² Guide to the CCSP CBK, Second Edition*.

Summary of Findings

Overall, we found that the Bureau has developed a life cycle process for deploying and managing security risks for Bureau systems, including for FedRAMP cloud systems used by the agency. However, the process is not consistently implemented for FedRAMP cloud systems used by the agency, and as such, it is not effective. For example, the Bureau has developed a security assessment and authorization (SA&A) process that is designed to identify and mitigate security risks for cloud systems throughout their life cycle. For four of the five FedRAMP cloud systems used by the Bureau, we found that this process was used. However, for one FedRAMP cloud system, which supports a key agency mission, we found that the Bureau had not ensured that its SA&A process was performed prior to system deployment. Specifically, we found that the Bureau deployed this FedRAMP cloud system without creating a comprehensive agency-specific security plan, performing an internal risk and security controls assessment, and granting an ATO. These processes are designed to ensure that CSPs have implemented security controls consistent with Bureau requirements and that any resulting risks are effectively managed.

We also identified opportunities to strengthen the Bureau's continuous monitoring processes for FedRAMP cloud systems once they have been deployed. Specifically, we found that the Bureau did not ensure that the PMO had an accurate inventory of the FedRAMP cloud systems used by the agency. The PMO relies on inventory information provided by agencies to ensure timely access to security-related information needed to perform effective continuous monitoring activities. Providing accurate FedRAMP inventory information to the PMO would enable the Bureau to identify and manage security risks in a timely manner. During our fieldwork, the Bureau took actions to develop and implement an automated workflow to help ensure that the PMO has an accurate inventory of the FedRAMP cloud systems used by the agency.

Lastly, we found that the Bureau does not verify electronic media sanitization performed by CSPs to ensure that affected agency data are rendered unrecoverable after a system reaches the end of its life cycle. Instead, the Bureau relies on attestations provided by CSPs that electronic media have been sanitized or destroyed according to contractual requirements. Obtaining additional assurance from CSPs, as appropriate, could further ensure that sensitive Bureau data are rendered unrecoverable at the end of a cloud system's life cycle.

Finding 1: The Bureau Should Consistently Use Security Assessment, Authorization, and Monitoring Processes to Manage Security Risks for Its FedRAMP Cloud Systems

We found that the Bureau has not consistently implemented its SA&A processes for deploying and managing risks for its FedRAMP cloud systems. Specifically, we found that the Bureau deployed a FedRAMP cloud system to support a key agency mission without completing its own risk assessment, developing a comprehensive security plan, or granting an ATO. We attribute this issue to an overreliance on vendor-provided security information and to operational priorities for implementing the system. Further, we found that the Bureau could improve its continuous monitoring activities for FedRAMP cloud systems it has deployed by gaining timely access to information provided by the PMO or the CSP and using that information to make risk-based decisions. Specifically, the Bureau did not ensure that the PMO had an accurate inventory of which cloud systems the agency was using and which it had decommissioned. This inaccurate inventory resulted in the Bureau not receiving comprehensive information with which to perform effective continuous monitoring of its FedRAMP cloud systems. By ensuring that SA&A processes are used to manage risks for cloud systems and that effective communication channels are maintained with the PMO, the Bureau will have more reliable and timely information with which to make risk-based decisions.

The Bureau Onboarded and Began Using a FedRAMP Cloud System Without Ensuring That Risks Were Comprehensively Assessed and Managed

We found that the Bureau onboarded and began using a FedRAMP cloud system to support the agency's Consumer Response Call Center processes without ensuring that its SA&A processes were followed to assess and manage agency-specific risks. Specifically, the Bureau had not developed a comprehensive system security plan (SSP), conducted an agency-specific risk and security controls assessment, or granted an ATO for the system prior to deploying it. This oversight presents a heightened security risk, as this cloud system supports processes for consumers who file complaints on financial products and services.

As noted earlier, one of the key benefits of FedRAMP is for agencies to reuse security authorization packages, including security plans, and to leverage the security assessments that have already been completed. To that end, the FedRAMP JAB provides a service whereby it will perform a risk review of security documentation submitted by a CSP and grant a provisional ATO. This provisional ATO is the JAB's recommendation to all federal agencies that a cloud system has a recommended acceptable risk posture

for the federal government to use at a designated impact level. In addition, an agency can perform a risk review of the documentation submitted by a CSP and grant a full ATO, which can also be leveraged by other agencies.

The *FedRAMP Security Assessment Framework* notes that if an agency decides to leverage an existing ATO issued by the JAB or another agency, as the Bureau did with the cloud system supporting Consumer Response Call Center processes, it still must issue its own ATO to accept the risk of using the system. Agency-specific risks may dictate that additional controls are required.

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 2 outlines key components of the Bureau's SA&A processes as they relate to system security planning, risk and security controls assessment, and ATO.

Table 2. Key Activities Supporting the Bureau's SA&A Processes

Activity	Requirement and description
System security planning	The SSP specifies the security requirements applicable to the system and the protection mechanisms implemented to meet those requirements. System owners are required to develop an SSP for each major information system.
Risk and security controls 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.
Authorization to operate	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 Policy* and *Risk Management Process*.

The Bureau deployed the FedRAMP cloud system to support Consumer Response Call Center processes without ensuring that SA&A activities were performed because of an overreliance on vendor-provided security information and operational priorities. Bureau officials also indicated that they were waiting for the CSP to complete planned system changes prior to performing an agency-specific risk assessment. 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.

The Bureau Did Not Ensure That Continuous Monitoring Activities Were Effectively Performed for Select FedRAMP Cloud Systems

After a system has been granted an ATO, the Bureau's SA&A process outlines continuous monitoring activities to oversee and monitor information security controls on an ongoing basis. These activities include coordinating with third-party providers and appropriate stakeholders, such as the PMO, to maintain situational awareness and manage risks to Bureau systems. We found that the Bureau did not have timely access to the FedRAMP ATO package, continuous monitoring reports, and security incident information for a FedRAMP cloud system it uses. The key cause for this lack of access was that the Bureau did not have a process to effectively communicate information to the PMO on the FedRAMP cloud systems it was using. As a result, we found that incident response time frames for one CSP were not specified in the CSP's incident response guide and may not align with Bureau practices. For another FedRAMP cloud system used by the Bureau, we identified that information system contingency plan testing had not been conducted in 2018 as required by the agency's information security policy. These issues, along with other potential deviations from Bureau security practices, could have been flagged through better oversight by the Bureau and effective information sharing with the PMO or the CSP, as appropriate.

The PMO maintains a central repository—the FedRAMP Marketplace—that lists the cloud service offerings that have been authorized for federal agency use, those currently in the authorization process, and those that have received the FedRAMP-Ready[5] status designation. Additionally, the marketplace lists which agencies are leveraging particular cloud systems and the associated FedRAMP ATO package. The PMO requires agencies to provide it with ATO letters when the agency begins using a FedRAMP-approved cloud. When an agency is no longer using a FedRAMP-approved cloud, the agency is responsible for communicating this information to the PMO. The PMO relies on the information on agency cloud ATO status and usage to provide agencies with timely access to key security documentation for the CSP providing the system. This documentation includes the FedRAMP ATO package, continuous monitoring reports, and security incident information.

In addition, the *FedRAMP Continuous Monitoring Strategy Guide* requires that agencies oversee the continuous monitoring activities of the CSPs they use by reviewing all security artifacts provided by the CSP or the PMO, as appropriate. With respect to incident reporting, the *FedRAMP Continuous Monitoring Strategy Guide* requires CSPs to annually provide information to the PMO on their incident response plan, including any updates that have been made. In addition, the guide requires CSPs to test and exercise their IT contingency plan at least annually and provide related deliverables to the PMO. The PMO makes this documentation available to agencies with ATOs on file.

Bureau officials stated that these issues resulted from a lack of formal policies, procedures, and resources to ensure effective communication with the PMO. We believe that by ensuring that the PMO has accurate information on the cloud systems used by the Bureau and strengthening continuous monitoring

[5] The FedRAMP-Ready designation is given to those systems or CSPs that have not yet undergone the FedRAMP authorization process.

processes for cloud systems, the agency will be able to better identify and prioritize the mitigation of security risks for the FedRAMP cloud systems it uses.

Management Actions Taken

While we were conducting fieldwork for this evaluation, the Bureau contacted the PMO to determine the procedures for maintaining the list of cloud systems used by the agency on the FedRAMP Marketplace and made updates to the listing. In addition, we observed that the Bureau established an automated workflow to ensure that system ATOs are being signed and routed to internal stakeholders and provided to the PMO, as appropriate. The PMO can use this information to maintain an accurate list of Bureau-used FedRAMP systems on the Marketplace. We confirmed that the Marketplace accurately reflected the FedRAMP systems used by the Bureau. As such, we are not making a recommendation in this area and will continue to monitor the Bureau's efforts to maintain an accurate inventory of its cloud systems as part of our future work under the Federal Information Security Modernization Act of 2014 (FISMA).

Recommendations

We recommend that the Chief Information Officer

1. Ensure that established SA&A processes are
    a. performed prior to the deployment of all FedRAMP cloud systems used by the Bureau.
    b. used to make an agency-specific authorization decision for the system that is in production and noted in our report.
2. Ensure that
    a. continuous monitoring information provided by the PMO or the CSP, as appropriate, is obtained and reviewed in a timely manner for all FedRAMP cloud systems used by the Bureau.
    b. for any gaps identified, including for incident response and contingency testing, a risk assessment is performed to determine appropriate responses.

Management Response

The Bureau's Acting Chief Information Officer concurs with these recommendations and notes that the agency has already begun the SA&A process for the system in question and anticipates that this process will be completed within 90 days of the issuance of this report. The Bureau has also deployed a tool to track and monitor the status of this SA&A process as well as to provide management visibility into all FedRAMP systems. Additionally, the Bureau has implemented a process for updating the FedRAMP Marketplace in a timely and accurate manner. Finally, the Bureau is working with its vendor to ensure that IT contingency planning testing is sufficiently tailored and updated to meet the agency's needs. The Bureau has developed a plan of action and milestones to track risks associated with the testing in question.

OIG Comment

We believe 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.

Finding 2: The Bureau Can Obtain Greater Assurance on the Effectiveness of Electronic Media Sanitization Performed by CSPs

We found that the Bureau could obtain additional assurance that CSPs are effectively sanitizing electronic media.[6] Specifically, we noted that the Bureau relies on CSP attestation as evidence that electronic media have been effectively sanitized. However, the Bureau's electronic media sanitization policy requires verification of media sanitization or destruction and disposal actions to ensure that agency data are rendered unrecoverable. Bureau officials informed us that they rely on the CSP to adhere to contractual requirements, as well as continuous monitoring activities performed by the PMO. However, as noted earlier, we identified opportunities to improve the Bureau's continuous monitoring approach for the FedRAMP cloud systems it uses. Obtaining greater assurance could assist the Bureau in ensuring that the CSPs are rendering Bureau data unrecoverable during media sanitization or destruction.

The Bureau Relies on CSP Attestation to Verify Electronic Media Sanitization

We found that the Bureau does not observe or verify the processes used by its CSPs to sanitize electronic media to render agency data unrecoverable when systems are decommissioned. For example, when the Bureau transitioned its Consumer Response System, which includes personally identifiable information, from one CSP to another, it did not observe or verify the effectiveness of the electronic media sanitization processes used by the original CSP. The Bureau did, however, receive a signed memorandum from the original CSP as an attestation that the locations where Bureau data were stored were permanently destroyed.

The *Bureau Media Sanitization and Destruction Standard* states that the system owner shall verify all media sanitization or destruction and disposal actions, including for parties operating on behalf of the Bureau. In addition, National Institute of Standards and Technology Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, notes that in a public cloud computing environment,[7] data from one consumer are physical collocated or commingled with the data of other consumers, which can complicate media sanitization processes. Further, in our *2018 Audit of the Bureau's*

[6] According to the National Institute of Standards and Technology, *sanitization* involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of media itself, to prevent unauthorized disclosure of information.

[7] As noted earlier, in a public cloud offering, different organizations share resources; however, their data remain isolated from that of the other organizations. Although the Bureau's data are isolated, we believe its data could be at risk for possible collocation or commingling.

Information Security Program report, we observe that Bureau officials are present when contractors perform media sanitization and destruction of physical data and hard drives maintained by the agency.[8]

Bureau officials informed us that the agency relies on CSP attestations of proper electronic media sanitization and data destruction as evidence that Bureau data are rendered unrecoverable. However, particularly in a public cloud environment where Bureau data could be collocated or commingled with the data of other organizations, we believe that the Bureau should evaluate obtaining additional forms of assurance. Obtaining greater assurance that electronic media storing Bureau data are effectively sanitized or destroyed by CSPs when no longer needed will help ensure that sensitive data are rendered unrecoverable at the end of a system's life cycle.

Management Actions Taken

While we were conducting fieldwork for this evaluation, the Bureau drafted new standard contract language that would require contractors, including CSPs, to provide certification that Bureau information on any non-government-furnished equipment has been sanitized in accordance with Bureau standards and procedures. Bureau officials stated that the updated contract language would be included in all new, future contracts; existing contracts would not be updated until renewal. These actions are a positive step to ensure that CSPs provide adequate assurance that electronic media sanitization activities render Bureau data unrecoverable upon system decommissioning. However, because the new standard contracting language does not apply to existing contracts the Bureau has with CSPs, we believe that the agency should evaluate other options to obtain additional assurance of electronic media sanitization or destruction and disposal performed by these providers for sensitive agency data. We will continue to monitor the Bureau's efforts in this area as part of our future FISMA reviews.

Recommendation

We recommend that the Chief Information Officer

3. Evaluate and implement, as appropriate, options to obtain additional assurance that electronic media sanitization performed by CSPs renders sensitive Bureau data unrecoverable when assets are decommissioned.

Management Response

The Bureau's Acting Chief Information Officer concurs with this recommendation and notes that for future system decommission efforts, the Bureau will assess the current state of the electronic media sanitization process performed by CSPs. Based on that assessment, the Bureau's Acting Chief Information Officer notes that the agency will create a plan to determine which additional artifacts will be sufficient to serve as confirmation and evidence that sensitive Bureau data are rendered unrecoverable for assets that are decommissioned.

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

OIG Comment

We believe 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.

Appendix A: Scope and Methodology

Our overall objective is to determine whether the Bureau has implemented an effective life cycle process for deploying and managing cloud systems that have been approved for federal agency use through FedRAMP. In addition, our objective includes determining whether the Bureau has implemented effective security controls for the FedRAMP cloud systems it uses. The first phase of our review focused on the effectiveness of the Bureau's life cycle and risk management processes for deploying and managing its FedRAMP cloud systems. Phase 2 of our review will focus on the effectiveness of security controls for select FedRAMP cloud systems used by the Bureau. The Bureau has deployed cloud systems that are not part of FedRAMP; those systems are not included in our scope.

To accomplish our objective, we (1) reviewed the roles and responsibilities of the FedRAMP PMO and the Bureau with respect to leveraging FedRAMP cloud systems and implementing and monitoring security controls, (2) analyzed the FedRAMP and Bureau-specific authorization packages for the FedRAMP cloud systems used by the Bureau, (3) assessed the Bureau's systems development and risk management processes for cloud systems, and (4) performed observation and testing of controls to meet requirements in the U.S. Department of Homeland Security's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* related to risk management, continuous monitoring, identity and access management, security training, configuration management, contingency planning, data protection and privacy, and incident response.

We performed our fieldwork from May 2018 to November 2018. We performed our evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B: Management Response

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

July 1, 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 C Streets, NW Washington, DC 20551

Thank you for the opportunity to review and provide comments on the Office of Inspector General's draft report *The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP*. We value your input and take seriously all concerns and recommendations made by your office.

We have reviewed your recommendations regarding strengthening the Bureau's processes for leveraging FedRAMP cloud systems in the areas of risk management, continuous monitoring, and electronic media sanitization. The Bureau agrees that strengthening these controls will ensure that our Cloud Service Providers (CSPs) have implemented security controls consistent with Bureau requirements, that the FedRAMP Project Management Office (PMO) has an accurate inventory of the cloud systems used by the agency, and that sensitive Bureau data are rendered unrecoverable at the end of the cloud system's lifecycle. Please be assured that the Office of Technology and Innovation (T&I) will continue to work towards addressing these recommendations.

Thank you for the professionalism and courtesy that you and your staff demonstrated during this review. Attached are our comments.

Sincerely,

KATHERINE SICKBERT

Digitally signed by KATHERINE SICKBERT
Date: 2019.07.01 09:03:07 -04'00'

Katherine Sickbert
Chief Information Officer (Acting)
consumerfinance.gov

Response to the recommendation presented in the Draft IG Report, "*The Bureau Can Improve the Effectiveness of Its Life Cycle Processes forFedRAMP*"

Recommendation 1: Ensure that established security assessment and authorization processes are

a) **performed prior to the deployment of all FedRAMP cloud systems used by the Bureau.**

b) **used to make an agency-specific authorization decision for the system that is in production and noted in our report.**

Management Response: The Bureau's Chief Information Officer concurs with this recommendation and notes that the Bureau has already begun the Security Assessment and Authorization (SA&A) process for the system in question and anticipates this process will be completed within 90 days of this report issuance. Additionally, CFPB has deployed our consolidated Cyber Security Assessment & Management (CSAM) tool to track and monitor the status of this SA&A process as well as provide management visibility into all FedRAMP systems. The established SA&A process currently identifies the final step as an agency-specific authorization decision for the system going into production.

Recommendation 2: Ensure that

a) **continuous monitoring information provided by the PMO or the CSP, as appropriate, is obtained and reviewed in a timely manner for all FedRAMP cloud systems used by the Bureau.**

b) **for any gaps identified, including for incident response and contingency testing, perform a risk assessment to determine appropriate responses.**

Management Response: The Bureau's Chief Information Officer concurs with this recommendation and notes that the Bureau currently has a newly-automated process for updating the PMO site in a timely and accurate manner prior to transitioning a system into ISCM and/or final decommission of system. The information for the system in question has also been updated and is now accurately reflected on the PMO site. Additionally, the cybersecurity organization is currently working with its vendor to ensure that Information Technology Contingency Planning (ITCP) testing is sufficiently tailored and updated to meet Bureau needs. The Bureau has opened a Plan of Actions and Milestones (POA&M) to track risks associated with the testing in question.

Recommendation 3: Evaluate and implement, as appropriate, options to obtain additional assurance that electronic media sanitization performed by CSPs renders sensitive Bureau data unrecoverable when assets are decommissioned.

Management Response: The Bureau's Chief Information Officer concurs with this recommendation and notes that for future system decommission efforts the Bureau will assess the current state of the electronic media sanitization process performed by CSPs and from that assessment will create a plan to determine which additional artifacts will be sufficient to serve as confirmation and evidence that sensitive Bureau data is rendered unrecoverable for assets that are decommissioned.

Abbreviations

ATO	authorization to operate
Bureau	Bureau of Consumer Financial Protection
CSP	cloud service provider
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
IaaS	infrastructure-as-a-service
IT	information technology
JAB	Joint Authorization Board
OIG	Office of Inspector General
PaaS	platform-as-a-service
PMO	Program Management Office
SA&A	security assessment and authorization
SaaS	software-as-a-service
SSP	system security plan
3PAO	third-party assessment organization

Report Contributors

Khalid Hasan, Senior OIG Manager for Information Technology
Andrew Gibson, OIG Manager, Information Technology
Kaneisha Johnson, Project Lead
Martin Bardak, IT Auditor
Emily Martin, IT Auditor
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