Open Recommendations Made to the Bureau of Consumer Financial Protection

We oversee the Bureau of Consumer Financial Protection by conducting audits, evaluations, and inspections of the Bureau's programs and operations and by making recommendations to improve economy, efficiency, and effectiveness.

Audits assess aspects of the economy, efficiency, and effectiveness of Bureau programs and operations and are conducted in accordance with *Government Auditing Standards*, which is issued by the comptroller general of the United States. Evaluations are generally focused on the effectiveness of specific programs or functions, and inspections are often narrowly focused on particular issues or topics and provide time-critical analyses. Evaluations and inspections are performed according to *Quality Standards for Inspection and Evaluation*, which is issued by the Council of the Inspectors General on Integrity and Efficiency.

Our audit, evaluation, and inspection reports explain why we conducted the review and the issues we found that should be corrected or improved, and they contain specific recommendations for agency corrective action. Table 1 shows, as of September 30, 2021, the total number and status of recommendations we made to the Bureau by calendar year, beginning with the first year for which recommendations remain open.

Table 1. Status of Recommendations for 2014–2021, as of September 30, 2021

Status	2014	2015	2016	2017	2018	2019	2020	2021
Recommendations	30	51	20	65	29	31	17	20
Open	1	0	0	2	6	8	8	20
Closed	29	51	20	63	23	23	9	0
Public recommendations	26	41	20	56	28	26	13	16
Open	1	0	0	2	6	7	4[a]	16[a]
Closed	25	41	20	54	22	19	9	0
Nonpublic recommendations	4	10	0	9	1	5	4	4
Open	0	0	0	0	0	1	4	4
Closed	4	10	0	9	1	4	0	0

Note: Some reports are restricted because they contain sensitive information. The recommendations from these reports are identified as nonpublic.

[a] Only the recommendations that have been open for more than 12 months are reflected in the accompanying list of open recommendations.

This document provides a list of publicly available report recommendations we made to the Bureau that have been open for more than 12 months as of September 30, 2021, and their status. The status designations and their definitions are as follows:

- Agency concurrence—The Bureau stated that it plans to implement the recommendation.
- Agency nonconcurrence—The Bureau stated that it does not concur with the recommendation. We continue to believe the recommendation should be implemented and are working with the Bureau to reach a resolution.
- Agency partial concurrence—The Bureau stated that it does not agree with part of the recommendation. We continue to believe the recommendation should be fully implemented and are working with the Bureau to reach a resolution.
- Agency action—The Bureau reported that it has begun taking steps to implement the recommendation.
- Partial implementation—The Bureau reported that it has completed actions to close part of the recommendation and is taking steps to close the remaining aspects.
- Verification in progress—The Bureau reported that it has completed actions to fully close the recommendation. We are verifying that the actions address the recommendation.

For inquiries about the list of open recommendations, please contact oig.media@frb.gov or 202-973-5043.

Publicly Available Bureau Recommendations Open for More Than 12 Months

Report title	Issuance date	Recommendation	Recommendation status
2014 Audit of the CFPB's Information Security Program 2014-IT-C-020	11/14/2014	3. 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.	Partial implementation
2017 Audit of the CFPB's Information Security Program 2017-IT-C-019	10/31/2017	1. Ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.	Partial implementation
		2. 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.	Agency action
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data 2018-MO-C-001	01/22/2018	2. Finalize the building access system upgrade to ensure that personal identity verification badges and site badges are automatically deactivated in the building access system and that personal identity verification badges are automatically deactivated in the USAccess system upon an individual's separation.	Partial implementation
		11. Once upgrades to the offboarding system have been fully implemented, develop a process to periodically reconcile new separation data in the offboarding system with one of the Bureau's human resources systems to ensure that the separation data are current, accurate, and complete.	Partial implementation
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program 2018-IT-C-003	02/14/2018	2. Develop, document and implement a formal process to monitor for compliance with physical security requirements around portable media such as laptops, thumb drives and smart phones, as well as passwords and hard copies of sensitive personally identifiable information.	Agency action
2018 Audit of the Bureau's Information Security Program 2018-IT-C-018	10/31/2018	1. Strengthen configuration management processes by a. remediating configuration-related vulnerabilities in a timely manner. b. ensuring that optimal resources are allocated to perform vulnerability remediation activities.	Agency action
		2. Develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.	Verification in progress

Report title	Issuance date	Recommendation	Recommendation status
		3. Determine whether established processes and procedures for management of user-access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.	Agency action
The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP 2019-IT-C-009	07/17/2019	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.	Partial implementation Part (b) of this recommendation is closed; part (a) remains open.
		2. Ensure that a. continuous monitoring information provided by the project management office or the cloud service providers, 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.	Agency action
		3. Evaluate and implement, as appropriate, options to obtain additional assurance that electronic media sanitization performed by cloud service providers renders sensitive Bureau data unrecoverable when assets are decommissioned.	Verification in progress
2019 Audit of the Bureau's Information Security Program 2019-IT-C-015	10/31/2019	2. Ensure that established security assessment and authorization processes are performed prior to the deployment of all cloud systems used by the Bureau.	Agency action
		3. Ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonpriveleged users.	Agency action
		5. Perform a risk assessment to determine a. the optimal deployment of the Bureau's technology for monitoring and controlling data exfiltration to all network access points. b. appropriate access to internet storage sites.	Agency action
		7. Ensure that system-level business impact analyses are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.	Verification in progress
Testing Results for Bureau's Plan of Action and Milestones Process 2020-IT-C-014	04/29/2020	1. Ensure that system owners are accurately estimating and accounting for costs associated with remediating security weaknesses listed in plans of action and milestones.	Agency action

Report title	Issuance date	Recommendation	Recommendation status
		2. Work with system owners to ensure that evidence to close system-level cybersecurity weaknesses listed in plans of action and milestones are submitted in a timely manner and that the weaknesses' status is accurately reflected in the Bureau's automated solution.	Verification in progress
Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program 2020-MO-C-018	08/17/2020	2. Develop a plan with measurable objectives to assess and monitor the Personnel Security Office's management of the background investigation process.	Agency action