

MANAGEMENT ALERT

CFPB: Hardware Assets at Former Regional Offices May Not Be Appropriately Secured



Introduction

The Consumer Financial Protection Bureau is responsible for regulating the offering and provision of consumer financial products and services under relevant laws. To conduct its work, the CFPB maintains databases containing millions of consumer complaints, sensitive financial information, and confidential supervisory records on financial institutions. Some of that information may reside on CFPB hardware assets, the loss of which could expose consumers' and businesses' private information, undermine public trust, and compromise the CFPB's ability to enforce consumer financial laws.

Objective, Scope, and Methodology

The Federal Information Security Modernization Act of 2014 (FISMA) requires the CFPB to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. FISMA also requires us to conduct an annual, independent evaluation to determine the effectiveness of the CFPB's information security program.

As part of our ongoing 2026 FISMA audit, we are evaluating the effectiveness of the CFPB's (1) security controls and techniques for sampled information systems and (2) information security policies, procedures, standards, and guidelines.

To accomplish our objectives, we reviewed the effectiveness of the CFPB's information security program across the core and supplemental metrics outlined in the Office of Management and Budget's *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. These metrics cover 10 security domains: cybersecurity governance, risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning. During our work, we found a potential security risk involving CFPB hardware assets that requires the CFPB's immediate attention. We are therefore issuing this management alert ahead of our full report. The information in this alert is based on testimonial evidence provided by CFPB officials.

We conducted this performance 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 obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The scope of our ongoing FISMA audit includes the CFPB's implementation of security controls to protect the confidentiality, integrity, and availability of its personally identifiable information and other sensitive agency data. The National Institute of Standards and Technology (NIST) outlines controls for agencies to use to protect physical and environmental systems, facilities, and hardware assets and to detect unauthorized hardware movement or removal.¹

In January 2025, the CFPB was leasing four regional offices from the U.S. General Services Administration (GSA). In February 2025, the CFPB and the GSA agreed to terminate the regional office leases, at which point the GSA assumed responsibility for the offices' physical security. However, the CFPB retained ownership and responsibility for the information technology (IT) assets that remained at these locations. According to a CFPB official, the CFPB stopped paying rent for its regional office leases that month and ceased paying fees for network connectivity in September 2025. As of March 2026, the CFPB had not completely vacated the regional offices.

The CFPB Cannot Validate the Security of Regional Hardware Assets

CFPB officials informed us that the agency left hardware assets at its former regional offices, which were vacated in 2025, and that occupancy and lease administration responsibilities for those former offices are managed by the GSA. The officials informed us that the CFPB retained ownership and responsibility for the IT assets that remained at these locations. They also informed us in June 2026, and reconfirmed in September 2026, that the CFPB has not verified whether those hardware assets, which the agency remains accountable for, are appropriately secured.

NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, requires organizations to enforce physical access authorizations at entry and exit points to the facility where hardware assets are located and to verify individual access authorizations before granting access.² It also requires organizations to employ asset-location

¹ National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5.

² National Institute of Standards and Technology, Special Publication 800-53, Revision 5, PE-3 (Physical Access Control).

technologies to track and monitor the location and movement of system components in controlled areas and to detect unauthorized movement or removal of organizational assets.³

The CFPB confirmed that, as of September 2026, it has no approved plan or time frame for verifying the security of hardware assets at former regional sites because of ongoing litigation and a lack of approvals to travel to these offices. By not verifying the security of these assets, which were left in four former regional offices over 18 months ago, the CFPB has no way of knowing whether the hardware assets, or the sensitive data that may be stored on them, have been accessed, modified, or removed by unauthorized individuals. As a result, the CFPB cannot verify the accuracy of its hardware asset inventory or confirm that assets at former regional sites remain secure and accounted for. We plan to include more information about this topic in our forthcoming 2026 CFPB FISMA report.

Recommendation

To ensure the security of hardware assets that may contain consumer complaint information, sensitive financial information, and confidential supervisory records and to ensure compliance with NIST physical security requirements, we recommend that the chief information officer

1. Ensure the hardware assets located at the former regional office spaces are appropriately accounted for and secured.

Agency Response and Our Evaluation

In response to our draft management alert, the CFPB concurred with our recommendation. The chief information officer stated that the CFPB has begun a full, site-by-site IT decommissioning of the former regional offices. The CFPB plans to follow a standardized, documented process to decommission the offices by September 30, 2026, and provide us with an update once complete.

The actions described by the CFPB appear to be responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed. The CFPB's full response is reproduced on the following pages.

³ National Institute of Standards and Technology, Special Publication 800-53, Revision 5, PE-20 (Asset Monitoring and Tracking).



September 18, 2026

Mr. Andrew Gibson III
Acting Assistant 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 Mr. Gibson,

Our response to the cited Management Alert and recommendation is below.

Sincerely,

CHRISTOPHER CHILBERT Digitally signed by CHRISTOPHER
CHILBERT
Date: 2026.09.18 08:52:20 -04'00'

Christopher Chilbert
Chief Information Officer

consumerfinance.gov

Response to recommendations presented in the OIG Management Alert: *CFPB: Hardware Assets at Former Regional Offices May Not Be Appropriately Secured*

Recommendation 1:

To ensure the security of hardware assets that may contain consumer complaint information, sensitive financial information, and confidential supervisory records and to ensure compliance with NIST physical security requirements, we recommend that the chief information officer

1. Ensure the hardware assets located at the former regional office spaces are appropriately accounted for and secured.

Management Response:

The Consumer Financial Protection Bureau concurs with the recommendation. The Bureau has already begun a full, site-by-site IT decommissioning of the former regional offices in New York, Chicago, San Francisco, and Atlanta, and network access to the sites was terminated in September 2025. The work to remove physical assets is being performed using the same standardized, documented processes that were successfully executed during the recent decommissioning of our former headquarters at 1700 G Street.

The Bureau emphasizes, however, that the Management Alert misapprehends the nature of the assets in those offices. Since we have a centralized data center and utilize cloud providers, the purpose of assets in the Regional Offices is primarily infrastructure, network/internet access, and administrative support such as audio-visual equipment. No databases containing sensitive data are housed in the regional offices. The Management Alert (at p. 3) claims otherwise: “This increases the CFPB’s vulnerability to data breaches and unauthorized disclosure of sensitive and confidential information.” Yet, it has no basis for this assertion. Nonetheless, as noted above, we are in the process of implementing the recommendation.

Our approach is to:

- Coordinate site access and logistics with building management and Physical Security
- Conduct a wall-to-wall inventory verification using our official asset inventory
- Sanitize and remove all data-bearing media in accordance with Bureau policy
- Teardown, reset, and remove all hardware assets
- Document chain-of-custody tracking for all hardware
- Dispose, transfer, or destroy assets using approved Bureau and GSA procedures and vendors
- Perform final reconciliation of asset states and disposition records

- Conduct daily cross-functional stand-ups to oversee planning, sequencing, and vendor coordination

This process ensures that each site is handled consistently and securely. All activities are expected to be completed by September 30, 2026. We will update when we conclude this set of activities.



Hotline

Report fraud, waste, abuse, and mismanagement involving the programs and operations of the Board or the CFPB.

oig.federalreserve.gov/hotline

OIG Hotline

Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

1-800-827-3340

General Contact

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

202-973-5000

Media and Congressional Inquiries

oig.media@frb.gov