

Banking and Finance Law Daily Wrap Up, PRIVACY—OIG finds CFPB's cybersecurity program is no longer effective, (Nov. 4, 2025)

Banking and Finance Law Daily Wrap Up

[Click to open document in a browser](#)

By Lauren Bikoff, MLS.

The report provided six new recommendations for the CFPB to strengthen its information security program.

In fiscal year 2025, the Consumer Financial Protection Bureau's procedures for securing its information systems have deteriorated, with the Bureau not maintaining authorizations to operate for many systems and using risk acceptance memorandums without a documented analysis of cybersecurity risks, according to a recent [audit](#) by the Office of Inspector General (OIG) for the Board of Governors of the Federal Reserve System and the CFPB. The OIG noted that this issue has been "compounded by the loss of contractor resources supporting information security continuous monitoring and testing activities and the departure of agency personnel." As such, the CFPB is "unable to maintain an effective level of awareness of security vulnerabilities in its environment," the audit report said.

The Federal Information Security Modernization Act requires the OIG to conduct an annual independent evaluation of the CFPB's information security program, practices, and controls for selected systems. Inspectors general must evaluate the agency's program on a maturity level (from a low of 1 to a high of 5). The 2025 fiscal year report found that the CFPB's overall information security program has decreased from a level-4 maturity (managed and measurable) in fiscal year 2024 to a level-2 maturity in 2025).

However, the OIG did find that the CFPB did take some steps to maintain and strengthen its information security program. For example, the agency updated and formalized processes for responding to potential ransomware incidents and transitioned toward a continuous vetting model for employee background reinvestigations. Additionally, the senior agency information security officer continues to meet with system owners on a weekly basis to manage cybersecurity risks, and the agency is in the process of decommissioning and modernizing legacy technology systems.

Recommendations. According to the OIG, eight previously made recommendations in the areas of data loss prevention, data classification, flaw remediation, and system/software inventorying remain open from previous years' audits. In the fiscal year 2025 report, the OIG provided the following six new recommendations in the areas of cybersecurity profiles, security authorizations, and information security continuous monitoring.

- (1) Determine what Enterprise Risk Management (ERM) roles, responsibilities, and strategy components should be defined and leveraged for the development and maintenance of cybersecurity profiles.
- (2) Develop and maintain cybersecurity risk registers to aggregate, normalize, and prioritize cybersecurity risks.
- (3) Develop policies and procedures to create and maintain cybersecurity profiles.
- (4) Perform a review of previously granted risk acceptance memorandums (RAMs) to determine whether they were based on a complete review of the system or common controls and perform additional risk analysis and/or implement compensating controls as needed for affected systems.
- (5) Ensure that RAMs reflect an assessment of qualitative and quantitative cybersecurity risks, as applicable.
- (6) Evaluate options to perform ongoing information continuous monitoring activities commensurate with the current threat environment.

The OIG stated that the CFPB concurred with the six new recommendations and outlined actions to address each recommendation.

MainStory: TopStory CFPB CyberPrivacyFeed DataPrivacy DataSecurity FinancialStability
OversightInvestigations Privacy