



**Office of Inspector General**

Board of Governors of the Federal Reserve System  
Bureau of Consumer Financial Protection

## MEMORANDUM

**DATE:** May 22, 2019

**TO:** Distribution List

**FROM:** Khalid Hasan   
Senior OIG Manager for Information Technology  
Office of Information Technology

**SUBJECT:** OIG Report 2019-IT-C-007R: Technical Testing Results for the Bureau’s SQL Server Environment

### Executive Summary

We are issuing this memorandum to bring to your attention weaknesses we identified in security controls for select Bureau of Consumer Financial Protection (Bureau) SQL Server instances and databases. Specifically, we identified that the security configurations for select SQL Server instances and databases were not aligned with established baselines and that significant weaknesses exist in controls for account management and configuration management. We identified these weaknesses as part of our *2018 Audit of the Bureau’s Information Security Program* report,<sup>1</sup> conducted pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). However, we did not include the specific details of these weaknesses in that public report because of the sensitive nature of the information.

We have reported similar weaknesses in our previous FISMA audits and in our system security control reviews. For example, in our 2014 FISMA report we made a recommendation to strengthen the Bureau’s vulnerability management practices related to web applications and databases; that recommendation remains open.<sup>2</sup> Also in 2014, our review of security controls for the Bureau’s cloud computing–based general support system included recommendations, which are now closed, to strengthen security controls for system and information integrity and configuration management.<sup>3</sup> In addition, our 2017

---

<sup>1</sup> Office of Inspector General, *2018 Audit of the Bureau’s Information Security Program*, [OIG Report 2018-IT-C-018](#), October 31, 2018.

<sup>2</sup> Office of Inspector General, *2014 Audit of the CFPB’s Information Security Program*, [OIG Report 2014-IT-C-020](#), November 14, 2014.

<sup>3</sup> Office of Inspector General, *Security Control Review of the CFPB’s Cloud Computing–Based General Support System*, [OIG Report 2014-IT-C-010](#), July 17, 2014.

## Distribution List

FISMA audit identified weaknesses in the Bureau's database systems related to passwords for system accounts, inadequate audit logging, and excessive privileges granted to users.<sup>4</sup>

We believe that the weaknesses we continue to identify heighten the risk of a breach of sensitive data maintained in the Bureau's SQL Server environment. As such, we are making five new recommendations to further assist the agency in its ongoing efforts to strengthen controls for its SQL Server instances and databases. These new recommendations cover specific technical controls and mechanisms that we believe should be strengthened for specific SQL Server instances and databases. We believe that by taking actions to address these new recommendations as well as the previously made recommendations, the Bureau can strengthen technical controls to better protect sensitive information maintained in its SQL Server environment.

---

<sup>4</sup> Office of Inspector General, *2017 Audit of the CFPB's Information Security Program*, [OIG Report 2017-IT-C-019](#), October 31, 2017.