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

MEMORANDUM

DATE: July 22, 2020

TO: Donna Roy
Chief Information Officer
Bureau of Consumer Financial Protection

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2020-IT-C-017R: *Technical Testing Results for the Bureau's Legal Enclave*

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 technologies that support the Legal Enclave. The Bureau's Legal Enclave includes systems and processes that are used to collect, store, process, and transmit critical information related to investigations and litigation (potential, anticipated, pending, or closed) for the Bureau.

Specifically, we found a significant weakness on a device that controls access to the environment housing the Legal Enclave, resulting in several security vulnerabilities. Further, the Bureau had not appropriately tested contingency planning activities for the device. In addition, we identified several security misconfigurations and security weaknesses for technologies in the Legal Enclave, which increase the risk of unauthorized data access and system misuse. Although the Bureau was aware of several of these issues, it had not taken timely action to mitigate the risks. The Bureau had accepted specific risks related to certain vulnerabilities in the Legal Enclave but had not formally documented its rationale for these decisions.

We identified these weaknesses as part of our *2019 Audit of the Bureau's Information Security Program*,[1] conducted pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). However, we did not include the specific details of these weaknesses in our public FISMA audit report because of their sensitivity. We have also reported similar technical configuration weaknesses and made

[1] Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*, OIG Report 2019-IT-C-015, October 31, 2019.

recommendations to strengthen related security controls in our previous Bureau FISMA audits and in our system security control reviews; several of those recommendations remain open.[2]

We believe that the weaknesses we continue to identify in Bureau technologies heighten the risk of a breach of sensitive agency data and system misuse. As such, we are making four additional recommendations in this memorandum to further assist the agency in its ongoing efforts to strengthen technical security controls. In its response to our draft report, the Bureau concurs with our recommendations and outlines actions that have been or will be taken to address them. We will follow up on the Bureau's actions to ensure that the recommendations are fully addressed. Given the sensitivity of our review, this report is restricted.

[2] 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; Office of Inspector General, *2014 Audit of the CFPB's Information Security Program*, OIG Report 2014-IT-C-020, November 14, 2014; Office of Inspector General, *2017 Audit of the CFPB's Information Security Program*, OIG Report 2017-IT-C-019, October 31, 2017; and Office of Inspector General, *Technical Testing Results for the Bureau's SQL Server Environment*, OIG Report 2019-IT-C-007R, May 22, 2019.