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

Executive Summary, 2018-IT-C-002R, January 25, 2018

Audit of the CFPB's Encryption of Data on Mobile Devices

Findings

We found that the Consumer Financial Protection Bureau (CFPB) currently has an effective process for encrypting the data on its mobile devices. The CFPB employs full-disk encryption on its laptops and a native encryption solution on its smartphones. We also found that the encryption methods employed by the CFPB meet federal requirements and that the agency uses adequate password complexity and reset rules.

Although the CFPB uses full-disk encryption for its laptop computers to ensure that sensitive data are not compromised if a laptop is lost or stolen, the CFPB has not been able to provide a full accounting of all laptops that have been assigned to users since the establishment of the agency. In June 2016, we issued an early alert memorandum to the CFPB in which we identified a number of steps that the agency should take to gain assurance that unaccounted-for laptops do not present an unacceptable level of risk to the agency and to strengthen technical controls over protecting sensitive data.

Since the issuance of our early alert memorandum, the CFPB has taken steps to assess the effect of the loss of the unaccounted-for laptops and strengthen controls for protecting sensitive data on mobile devices. We found, however, that the CFPB has not completed all the steps outlined in our early alert memorandum related to the data access actions of individuals to whom the unaccounted-for laptops were assigned.

We believe that integrating specific activities for managing the risk posed by sensitive data on unaccounted-for laptops, such as role-based analysis and system log reviews, will strengthen the CFPB's ongoing efforts to develop and implement an insider threat program and incident containment strategies.

In his response to our draft report, the Chief Information Officer concurs with our suggestion and notes that the CFPB will incorporate it as part of the agency's efforts to evolve its insider threat program and mature its information technology asset management program. We will continue to follow up on the CFPB's actions to strengthen its information technology asset management practices, develop its insider threat program, and implement incident containment strategies as part of future audits of the CFPB's information security program.

This report is restricted due to the sensitive nature of this information.

Purpose

The CFPB provides mobile devices to its staff members to help them carry out their duties. The portability of these devices brings a heightened risk of loss or theft of the devices as well as compromise of sensitive information stored on the devices. Our objectives were to evaluate (1) the effectiveness of the CFPB's techniques for encrypting data on mobile devices and (2) the strength of the encryption methods and the password complexity and reset rules applied.

Background

We initiated this audit because of identified deficiencies in the CFPB's inventory management processes for laptop computers. Specifically, the U.S. Government Accountability Office identified a significant deficiency in the CFPB's inventory controls for information technology assets, including laptops, as part of its fiscal year 2015 financial statement audit. In addition, our prior years' audits of the CFPB's information security program addressed the need for (1) inventory controls over information technology assets; (2) an agencywide insider threat program that integrates incident response capabilities; and (3) containment strategies for the key types of incidents applicable to the agency's environment, including those involving the loss or theft of equipment as an attack vector.