




OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

DEC 21 2015

Memorandum

To: Sylvia Burns
Chief Information Officer
U.S. Department of the Interior

From: Mary L. Kendall 
Deputy Inspector General

Subject: Management Advisory – Failure To Adequately Protect Sensitive Data on
Thousands of U.S. Department of the Interior Laptop Computers
Report No. ISD-IN-MOA-0004-2014-H

In this advisory, we focus on the efficacy of the U.S. Department of the Interior's (Department) measures for protecting sensitive data on its laptop computers from unauthorized access. We found that a management decision to depart from a recognized best practice put sensitive data on almost 15,000 laptops Departmentwide at high risk of compromise if the devices are lost or stolen. The extent of the potential security breach is not limited to sensitive data on a lost or stolen laptop. For example, a cybercriminal in possession of one of the thousands of Department laptops could use data stored on it, such as usernames and passwords, to gain unauthorized access to the Department's computer networks and systems.

Background

The Department has issued tens of thousands of mobile computing devices to its employees and contractors, including a large number of laptop computers. Many of these laptops process and store sensitive data related to bureau programs and operations and also contain personally identifiable information (PII) such as Social Security numbers for Department employees. In addition to sensitive data on departmental programs and PII, laptops also store cached usernames and passwords used to access Department computer networks and systems. Thus, the Department must implement measures to protect sensitive data on its laptops from unauthorized access in the event that devices are lost or stolen. In fact, a leading information technology (IT) security firm found that lost or stolen mobile computing devices, including laptops, tablet computers, and smartphones, were the leading cause (41 percent) of reported data breaches from 2005 to 2015.¹

The Department has a variety of options available to help prevent unauthorized access to data stored on its laptop computers. These include password protecting computers, encrypting individual files, or encrypting computer hard drives, which is commonly referred to as full-disk or whole-disk encryption. Password protecting a computer using the machine's operating system

¹ TrendMicro Inc., "Follow the Data: Dissecting Data Breaches and Debunking the Myths," September 22, 2015.

is the least effective way to prevent unauthorized access because it is relatively easy for hackers to bypass a computer's logon/password screen and gain full access to stored data. Encrypting individual computer files prevents unauthorized access to those files, but requires ongoing awareness and a proactive effort by the user to identify and encrypt specific files. In contrast, full-disk encryption encrypts all data and programs on the computer and automatically encrypts new data and programs as they are added. Because of this, full-disk encryption is the most effective way to ensure that sensitive information is not compromised if a laptop is lost or stolen. The Department selected full-disk encryption as its solution for protecting data on its laptops and installed McAfee's full-disk encryption software on all of its laptops by the end of 2011.

Like any other security control, full-disk encryption must be implemented correctly in order to be effective. For example, full-disk encryption software can be configured for pre- or post-boot user authentication. For pre-boot authentication, the user is presented with a login screen when the laptop is powered on—before the computer's operating system and encryption key are loaded into memory. Upon successful pre-boot authentication, the laptop's operating system is loaded and the user authenticates with a username and password or PIV card and PIN a second time before gaining access to the laptop's data and programs. Conversely, the user authenticates once for post-boot authentication—after the operating system and encryption key are loaded into memory.

Users typically prefer post-boot authentication because they only need to login once to access files and programs on their laptops. If only post-boot authentication is used and the laptop is lost or stolen, then the laptop is vulnerable to a direct memory access attack, which is a highly effective form of cyberattack originally discovered in 2004 with widely released exploits since 2008.² In a direct memory access attack, the attacker uses free software programs in conjunction with a special network card and cable (total cost of approximately \$30) to extract the laptop's encryption key from memory. This process only takes about 15 minutes. The attacker then uses the stolen encryption key to decrypt the laptop's hard drive. Once decrypted, the attacker has full access to all sensitive data stored on the laptop. This includes cached usernames and passwords, which the attacker can potentially use to gain unauthorized access to an organization's computer networks and systems. For these reasons, the National Institute of Standards and Technology recommends that organizations use pre-boot authentication when implementing full-disk encryption.³ Moreover, pre-boot authentication is the default setting for McAfee's full-disk encryption software installed on Department laptops.

Finding

As part of our "Evaluation of the Cyber Security of the Department's Mission-Critical Information Technology Systems" (No. ISD-IN-MOA-0004-2014), we evaluated selected IT security controls to determine whether the controls were implemented correctly, operating as intended, and producing the desired outcome of protecting Department computer systems and data. We found that as of August 27, 2015, nearly 15,000 encrypted laptop computers

² <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1038> and <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-1038>

³ National Institute of Standards and Technology, Special Publication No. 800-111, "Guide to Storage Encryption Technologies for End User Devices," November 2007.

Departmentwide did not use pre-boot authentication, potentially exposing any sensitive data stored on them to unauthorized access through direct memory access attacks if the laptops were lost or stolen. Moreover, the extent of the potential IT security breach is not limited to sensitive data on a lost or stolen laptop. For example, a cyber attacker in control of one of the thousands of laptops could potentially use data stored on it, such as cached usernames and passwords, to gain unauthorized access to the Department's computer networks and systems. Once inside the Department's computer network, the cyber attacker could potentially disrupt bureau operations and steal sensitive data. Thus, the Department's ineffective implementation of full-disk encryption could not only result in the loss of sensitive data on a compromised laptop, but could also be used to breach bureau networks and systems, potentially resulting in severe adverse effects on Department IT assets, operations, and individuals. This control deficiency occurred because bureau officials changed the default setting on the Department's encryption software from pre- to post-boot authentication without conducting a valid risk assessment.

On August 20, 2015, we provided a briefing to the Department's Office of the Chief Information Officer and the Bureau Assistant Directors of Information Resources to introduce this finding and request additional information regarding the extent and possible impact. The briefing included detailed information regarding the processes and tools we used to successfully decrypt sample hardware provided by the Department. The Department reported that 14,426 of 40,695 (35 percent) laptops across all bureaus and offices were not configured to require pre-boot authentication. Over the last 3 years, the Department has documented 64 incidents in which laptop drives were lost or stolen without pre-boot authentication enforcement. As of November 16, 2015, the Department has reduced the number of misconfigured laptops to 11,593.

Recommendation

We recommend that the Department's Chief Information Officer mandate the use of pre-boot authentication on all laptops and implement a monitoring and enforcement program that mitigates noncompliant systems.

Response Required

Please respond to this management advisory within 30 days. Your written response should provide detailed information on the actions you have taken, or plan to take, to address our recommendation, as well as target dates and titles of officials responsible for implementing these actions. Please address your response to:

Kimberly Elmore
Assistant Inspector General for Office of Audits, Inspections, and Evaluations
U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW.
Mail Stop 4428-MIB
Washington, DC 20240

If you have any questions regarding this management advisory, please contact me at 202-208-5745.