LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Angus Maciver

# MEMORANDUM

| | |
|---|---|
| **TO:** | Legislative Audit Committee Members |
| **FROM:** | Aubrey Curtis, Information Systems Auditor |
| **CC:** | Tim Fox, Attorney General, Department of Justice<br>Pam Bucy, Commissioner, Department of Labor and Industry<br>Richard Opper, Director, Department of Public Health and Human Services<br>Mike Kadas, Director, Department of Revenue |
| **DATE:** | June 2013 |
| **RE:** | Information Systems Audit Follow-up 13SP-10: Improving Controls Over Security of Laptop Data (orig. 11DP-12) |
| **ATTACHMENTS:** | Original Information Systems Audit Summary |

## Introduction

The information systems audit *Improving Controls Over Security of Laptop Data (11DP-12)* was issued to the Committee in January 2012. The purpose of the audit was to review a sample of laptops from four state agencies (Justice, Labor and Industry, Public Health and Human Services, and Revenue) to assess whether proper controls were in place to protect sensitive information contained on those systems. In May 2013, we conducted follow-up work to determine whether recommendations were implemented. This memorandum summarizes our follow-up findings.

**Overview**

Our testing of security controls at the four agencies identified laptops that were vulnerable to potential security breaches. The audit report contained three recommendations for improving security controls, including periodic monitoring of security settings, improving user awareness, ensuring encryption, and analyzing need for laptops. Each agency did concur with and is currently working on implementing its respective recommendations.

## Background

Agencies should implement data security controls that meet minimum requirements and guidelines established in statute, policy, and best practices. For this audit, our objective was to determine if security controls were in place to protect any and all sensitive information on laptops. We identified key controls that should be in place to ensure necessary security and developed a testing protocol to verify the existence of controls. We tested 100 laptops at the four agencies and identified laptops within all four agencies that had security vulnerabilities.

## Follow-Up Audit Findings

The following sections summarize progress towards implementing the report recommendations. We combined all four agencies into each recommendation summary. The implementation status for each recommendation is the least implemented of the combined agencies.

**RECOMMENDATION #1**

**We recommend the agencies:**

**A. Routinely monitor laptop security settings to ensure application of security controls.**
**B. Improve and maintain user awareness of laptop security policies and procedures.**

**Implementation Status Being Implemented**

Since our audit, each agency has taken steps towards improving continued monitoring of laptops, along with increased security awareness training for all personnel (specifically those utilizing mobile devices). The Department of Justice (DOJ) now uses Microsoft Configuration Manager to centrally manage mobile devices, which includes maintaining security settings and deployment of automatic updates and patches. With this new tool, the number of laptops the agency is able to remotely monitor increased. The Department of Public Health and Human Services (DPHHS) is using Configuration Manager software as well, while the Department of Revenue (DOR) is using a similar capability with Windows Server Update Services. The Department of Labor and Industry (DOLI) has taken a more hands-on approach by physically inspecting all laptops and mobile devices deployed to locations around the state. DOLI Information Technology (IT) staff developed a security checklist which is completed on the systems during these visits. All agencies have placed an emphasis on information security by integrating security awareness into employee training for all personnel. Most have updated their new employee orientation curriculum to include this information as well.

**RECOMMENDATION #2**

**We recommend the Department of Labor and Industry, Department of Justice, and Department of Revenue take steps to ensure compliance with state policy by implementing or improving procedures to ensure sensitive data on laptops is encrypted.**

**Implementation Status Being Implemented**

At the time of the audit, DPHHS was encrypting all data through full hard drive encryption. As a result, the audit report did not address this recommendation to DPHHS. DOR now has Symantec Endpoint Encryption on approximately 98.5 percent of its laptops. The remainders are users who are exempt due to job requirements, for which they signed exception letters. DOLI is conducting sensitive data assessments on laptops and other mobile devices and maintains documentation of all users storing sensitive information such as personally identifiable information (PII). IT staff use this data to determine which systems will require encryption software, TrueCrypt. The agency has not encrypted all systems containing PII, but it has addressed laptops of key personnel and is working towards installation of TrueCrypt on all laptops. DOJ is making an initial push to require all employees to save documents to network drives. Eventually, the agency's plan is to implement a virtual environment for all laptops which will be controlled centrally and force users to save files to network drives.

**RECOMMENDATION #3**

**We recommend the agencies analyze business need, security risk, and cost-effectiveness prior to assignment of laptops.**

**Implementation Status Being Implemented**

From an IT perspective, this recommendation is being implemented. IT personnel within all four agencies continue to stress to program managers the information security risk involved with employees using laptops. However, the authority of determining need for laptops still resides with program managers and supervisors, and it is their decision whether or not to assume that risk. During our follow-up work, we did not receive information indicating agencies have changed processes related to analysis of business need or cost-effectiveness prior to issuing laptops to employees.