

INFORMATION SYSTEMS AUDIT
Improving Controls Over Security of
Laptop Data

Department of Justice, Department of Labor and
Industry, Department of Public Health and Human
Services, Department of Revenue

JANUARY 2012

11DP-12

REPORT SUMMARY

Laptops comprise almost 25 percent of all computers used in Montana state government. Laptops provide for added mobility, but they also present an increased risk to data security. Current controls do not ensure an adequate level of security for all data within the departments reviewed.

Context

During recent years, use of laptop computers within state government has steadily increased. The 2011 Biennial IT Report states laptops make up 23 percent of all computers compared with 14.6 percent for the previous biennium. Overall, the State Information Technology Services Division reports 3,431 laptops in service throughout state government, excluding the university system. Reasons for the rise in laptop use are their portability and ability to connect remotely to the state network. This provides laptop users the flexibility to travel for work and maintain communication with their offices.

While laptops allow for added mobility and flexibility, they also present added data security risks. Because they are portable, laptop computers are often outside the physical security of state offices and at risk of loss or theft. This becomes critical when laptops are used to service and store confidential data, increasing the need for added physical and data security. Because of the heightened security risk, we conducted an audit to identify and test laptop security controls to verify security

of sensitive data. To achieve our objective, we developed testing protocol based on statute, best practices, and state policy and tested a sample of 100 laptops at four different agencies.

Results

Overall, we identified laptops throughout all four agencies that are vulnerable to potential security breaches. We issued recommendations for agencies to improve security controls, including periodic monitoring of laptop security settings, improving user awareness of security policies and procedures, ensuring encryption of sensitive laptop data, and limiting the use of laptops.

Recommendation Concurrence	
Concur	3
Partially Concur	0
Do Not Concur	0
Source: Agency audit response included in final report.	

For a complete copy of the report (11DP-12) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to lad@mt.gov; or check the web site at <http://leg.mt.gov/audit>
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail lad@mt.gov.