MONTANA LEGISLATIVE AUDIT DIVISION

INFORMATION SYSTEMS AUDIT
Photocopier Data Security
Department of Administration

MAY 2012 12DP-01 REPORT SUMMARY

Photocopiers can have hard drives just like computers, and thus may store sensitive and confidential data internally. If not properly controlled, there is potential for unauthorized access to this data. Although, we did not identify any data security breaches, there is a lack of awareness of data security controls.

Context

Photocopiers are standard equipment in many state offices. Copiers in today's office can be multi-function devices that not only copy, but also print, scan, fax, and email all types of office information, including sensitive and confidential data. Since the early 2000's, most digital copiers have a hard drive, just like a computer. For a copier with a hard drive, data is stored internally. If this data is not removed from the hard drive or the hard drive destroyed when a copier is removed from service, sensitive data may be released to unauthorized individuals. For example, a news story released in 2010 identified federal surplused copiers with sensitive data still stored on hard drives. State IT policy requires all electronic data storage devices to have all data removed so it cannot be recovered (sanitized) or physically destroyed prior to disposal. State IT policy further requires agencies to maintain documentation of the disposal of these devices.

Results

We reviewed settings on 31 copiers to identify where the data is stored and what data protections were in place. Of those, seven copiers stored data on internal hard drives. Three of these require a username and password for data access, while data on the other four copiers is accessible by anyone on the same network.

While reviewing Department of Administration contracts for completeness we identified areas for strengthening contract language. For 15 agency locations outside of Helena, individuals responsible for copiers at 8 were not aware of any policy regarding copier hard drive disposal and 5 believed copier vendors, not agencies, are responsible for hard drive disposal. Furthermore, of nine reviewed agencies, three do not track sanitized/disposed hard drives.

Overall, we did not identify any copier data security breaches but noted controls could be strengthened. We noted some agency personnel are not aware of, or following, state IT policy. Using existing IT groups would facilitate awareness of photocopier data security policy and controls.

Recommendation Concurrence	
Concur	2
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

For a complete copy of the report (12DP-01) 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.