

Testimony of Senator McGee
Before the Senate State Administration Committee
Senate Bill 148

Madam Chair, members of the committee, for the record my name is Dan McGee,

Senator from Senate District 29. It is my pleasure to introduce to you SB148, a bill known as the Criminal Records Checks for IT Professionals Act.

I think all of us have become keenly aware of how computer systems, and the data they process, play a crucial role in conducting the business of the state and in providing needed services to Montana citizens. However these powerful tools, in the wrong hands, can be used to steal identities, perpetrate fraud against the State or citizens, or invade the privacy of individuals. There are countless stories, from both the public and private sectors, of misuse of systems or data.

Information Technology systems within the State of Montana support the full range of program functions of state agencies. Whether the state is paying a bill or a benefit; processing a benefits claim or tracking diseases; preparing a criminal case or processing a tax return, computer systems and sensitive data are essential to those processes. In recent years we have become more aware of requirements imposed by the FBI, by the IRS, and by HIPPA (the Health Information Portability & Privacy Act) that our information technology assets be safeguarded.

State agencies have done a very good job implementing solid system security practices and system features to safeguard our State IT assets. Examples include user authorization controls and audit trails, and preventing intrusions by outsiders.

The Legislative Auditor places heavy emphasis on those security features to minimize any risk of system misuse and to ensure privacy and protection of data pertaining to you, me, and the rest of Montana's citizens.

Despite the security measures used, there is still the need to trust a number of state employees to not abuse or misuse the systems and data. That group consists of our IT employees who administer the systems and manage the data. By virtue of the requirements of their jobs, many IT employees have comparatively unfettered access to a wide range of critical systems and sensitive data. It speaks well of their integrity that there have been no incidents of misuse or inappropriate behavior on their part. However, we owe it to the citizens of Montana, and the federal mandates, to go beyond just blind trust. We need to assess whether members of our IT staffs have any criminal behavior in their backgrounds that presents an unacceptable risk for misbehavior in the future.

This act allows us to go beyond blind trust. Simply put, it requires state agencies to perform background checks on IT employees, including contractors, whose jobs put them in a position of trust. To a limited extent this is being done already for some employees in the Department of Justice and the Department of Administration, Information Technology Services Division, who have positions of trust related to the Criminal Justice Information System. This bill extends background checking to other settings where sensitive systems and data are managed.

The cost per affected IT staff member or proposed contract worker is estimated at less than \$50 and will be the responsibility of the agency employing the staff member

or, in the case of contractors, the contracting firm through a reimbursement to the agency. This is an insignificant cost when considered in comparison to the damage that result from inappropriate use of systems or data.

It's important to understand that this act requires the involved agency management to make the tentative determination whether any negative findings in the employee's, or candidate's, or proposed contractor's background requires personnel action. State and federal employment law guide those actions. Tentative disposition options include retention or hire, transfer, demotion, or dismissal. Tentative dispositions will be reviewed by the department of Administration and either accepted or rejected.

In summary, this act reduces the risk that IT employees in positions of trust will misuse their unique access privileges by giving state officials the ability to avoid putting high risk people in those positions.

In summary, this act reduces the risk that IT employees in positions of trust will misuse their unique access privileges. By requiring state officials to identify people with high-risk backgrounds, they will avoid putting State systems and data in needless jeopardy.

I ask for your favorable consideration of this bill. At this point I would like to turn the podium over to Jeff Brandt, Acting State CIO, for further comments and to address questions of the committee.

I reserve the right to close.

Thank you.