SUMMARY

The Office of the Auditor General has conducted a special review of the Financial Management Information System (FMIS) Disaster Recovery management pursuant to Title 12 NNC § 2.

FINDING I. Lack of a comprehensive FMIS disaster recovery plan

The Office of the Controller (OOC) did not develop a comprehensive disaster recovery plan that will meet the general requirements of continuing business if disaster occurs, for instance, fire, in-house flooding, sabotage, physical theft, technology and security intrusions, and hardware failures.

FINDING II. A comprehensive inventory list of FMIS information technology software for disaster recovery is not maintained.

The OOC does not maintain a complete and accurate inventory of the FMIS software assets for disaster recovery. The OOC will be unable to accurately identify the critical software components of the FMIS operations in a timely manner if a disastrous event occurred.

FINDING III. Lack of Certified FMIS Computer Hardware for Disaster Recovery.

The OOC does not maintain an accurate and complete listing of FMIS computer and network infrastructure equipment for disaster recovery. The inventory list is necessary to rebuild the FMIS computing operations if a disaster occurs.

FINDING IV. Funding of a disaster recovery program is not adequate.

The OOC operating and fixed cost budgets for fiscal year 2008 and 2009 do not include costs or contingency plans for disaster recovery activities other than computer system backups. There are no budget policies in place to assure major FMIS users that their operations are not jeopardized and placed at risk after a disaster occurrence.

FINDING V. Lack of service level agreements with major FMIS users.

The OOC did not provide service level agreements with major FMIS users that define customer requirements and information technology capabilities. Disaster recovery activities such as planning, consultation, assurances and/or coordination efforts are lacking or non-existent with major FMIS users.

FINDING VI. The FMIS data center is not adequately protected.

The FMIS data center is not adequately safeguarded in the event of a fire. There is a lack of adequate fire protection and detection equipment at the FMIS computer equipment premises that is in accordance with information technology standards.

FINDING VII. There is no assurance that the FMIS information technology equipment is properly insured.

The OOC did not submit the 2010 Risk Management Property Schedule listing in detail the FMIS computer equipment and the purchase costs, fair market value or replacement costs. Consequently, there is no verifiable computer equipment listing to be used for insurance claims and recovery in the event of equipment losses.