Office of MN.IT Services' Data Centers

Information Technology Controls and Compliance Audit

As of November 2016

March 2, 2017
REPORT 17-06

Financial Audit Division

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Office of the Legislative Auditor
Financial Audit Division

The Financial Audit Division at the Office of the Legislative Auditor (OLA) performs three types of audits of entities within the state's executive and judicial branches:

- **Financial Statement** audits determine whether an entity has prepared its Comprehensive Annual Financial Report in accordance with governmental accounting principles. The division provides audit opinions on the financial reports for the State of Minnesota, the state's three large public pension plans, and the Minnesota Sports Facilities Authority.

- **Federal Grant Compliance** audits determine whether the state has complied with federal requirements for many of its largest federal programs. Often called the *Single Audit*, the federal government requires these audits as a condition of receiving federal grants.

- **Internal Controls and Legal Compliance** audits determine whether an entity has internal controls to effectively manage the risks of its financial operations and whether it has complied with legal compliance requirements chosen for testing.

The Financial Audit Division has a staff of about 35 auditors, many of whom are licensed CPAs and hold other certifications. The division conducts its audits in accordance with *Government Auditing Standards* established by the Comptroller General of the United States.

One requirement of the audit standards is a periodic review of the division's system of quality control by audit peers from across the country. The division's most recent peer review report is available at: www.auditor.leg.state.mn.us/fad/pdf/fadpeer.pdf

---

OLA also has a **Program Evaluation Division** that evaluates topics periodically selected by members of the Legislative Audit Commission.

In addition, OLA may conduct a **Special Review** in response to allegations and other concerns brought to the attention of the Legislative Auditor. The Legislative Auditor conducts a preliminary assessment in response to each request for a special review to determine what additional action, if any, OLA should take.

OLA
OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

March 2, 2017

Senator Mary Kiffmeyer, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Thomas Baden, Commissioner and Chief Information Officer
Office of MN.IT Services

This report presents the results of our information technology controls and compliance audit of the Office of MN.IT Services' data centers as of November 16, 2016. The objectives of this audit were to determine if the Office of MN.IT Services had adequate internal controls to provide reasonable assurance that it protected the physical access and operational environment of the computer equipment, networking systems, and components in its enterprise data centers and the agency-based data centers we tested.

We discussed the results of the audit with the office's staff at an exit conference on February 22, 2017. This audit was conducted by Michael Anderson, CPA, CISA (Information Technology Audit Director) and Michael Fenton, CISA (Information Technology Audit Coordinator).

We received the full cooperation of the office's staff while performing this audit.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor


THE GREAT SEAL OF THE STATE OF MINNESOTA
L'ETOILE DU NORD
1858

Table of Contents

Page

Report Summary 1

Agency Overview 3

Objectives, Scope, and Methodology 4

Conclusion 6

Findings and Recommendations 7

1. The Office of MN.IT Services did not have adequate physical or environmental controls for some of the agency-based data centers it operates 7

2. The Office of MN.IT Services did not update or test the contingency plan for the enterprise data centers in a timely manner 8

Office of MN.IT Services' Response 11


THE GREAT SEAL OF THE STATE OF MINNESOTA
L'ETOILE DU NORD
1858

Report Summary

The 2011 Information Technology Consolidation Act consolidated the state's information technology resources under the direction of the State Chief Information Officer in the Office of MN.IT Services.[1] The Office of MN.IT Services (MN.IT) is an executive branch agency that provides information technology services to other state agencies. Since 2011, MN.IT has been working to consolidate the computer operations for state agencies into enterprise data centers, which will serve multiple agencies.[2] As of November 2016, MN.IT had reduced the total number of data centers from 49 to 28.

We conducted this audit to determine whether MN.IT had adequate controls in place to protect data center facilities and the computing equipment contained in them.

Conclusion

The Office of MN.IT Services had generally adequate information technology controls to provide reasonable assurance that it protected the physical access and operational environment of the computer equipment, networking systems, and components in its enterprise data centers and the two agency-based data centers we tested. The Office of MN.IT Services also generally complied with related applicable state and federal legal requirements and MN.IT policies and procedures we tested.

However, the Office of MN.IT Services had some weaknesses related to the operation of agency-based data centers and the updating, testing, and training for the disaster recovery plan for the enterprise data centers.

Audit Findings

- The Office of MN.IT Services did not have adequate physical or environmental controls for some of the agency-based data centers it operates. (Finding 1, page 7)
- The Office of MN.IT Services did not update or test the contingency plan for the enterprise data centers in a timely manner. (Finding 2, page 8)

[1] *Laws of Minnesota* 2011, First Special Session, chapter 10, art. 4, sec. 6.

[2] MN.IT did not receive funding to help accomplish the data center consolidation goals that policymakers anticipated in the 2011 legislation. As a result, MN.IT has relied on one-time contributions from agencies to fund the data center migrations that have been completed to date.


THE GREAT SEAL OF THE STATE OF MINNESOTA
L'ETOILE DU NORD
1858

Agency Overview

Office of MN.IT Services

The Information Technology Consolidation Act, passed in the 2011 Special Session, consolidated the information technology resources of executive branch agencies under the direction of the State Chief Information Officer in the Office of MN.IT Services. The Office of MN.IT Services (MN.IT) is an executive branch agency that provides information technology services to other state agencies.

Through consolidating the information technology operations of agencies, boards, and commissions, it was the intent of the Legislature and the Governor to improve the effectiveness and efficiency of the delivery of information technology services in meeting the business needs of state government and increase the potential for technology-driven improvements to government services.[3]

A data center houses the computer equipment and networking systems and components for an organization's information technology needs. In addition to housing the computer equipment and networking systems and components, data centers provide physical and environmental controls to support the operation of the computer systems.[4]

A large enterprise data center allows an organization to co-locate computing equipment used by a variety of entities in an environment with continuous monitoring of access to the facility and equipment; duplicate power feeds from the public utility; on-site emergency generators; on-site uninterruptible power supply equipment to protect the information systems against power spikes and power outages; and duplicate systems for cooling, water detection, and fire detection and suppression.

At the time of the Information Technology Consolidation Act, the various state agencies had 49 data centers, primarily designed to serve the needs of the individual agencies. MN.IT has been working towards consolidating these agency-based data centers into enterprise data centers, which will serve multiple agencies.[5] By consolidating the agency-based data centers into enterprise data

[3] *Laws of Minnesota* 2011, First Special Session, chapter 10, art. 4, sec. 6.

[4] Examples of physical and environmental controls for data centers include restrictions on access to the facilities; monitoring of access to the facilities; monitoring of the operation of computer equipment and air conditioning/temperature equipment; power supplies backed up by external generators; uninterruptible power supply equipment to protect against power spikes and outages; raised flooring and water detection devices; and fire detection and suppression systems.

[5] MN.IT did not receive funding to help accomplish the data center consolidation goals that policymakers anticipated in the 2011 legislation. As a result, MN.IT has relied on one-time contributions from agencies to fund the data center migrations that have been completed to date.

centers, MN.IT can better protect the state's information systems equipment and reduce the risk of information systems' process disruptions.

MN.IT established two enterprise data centers and is in the process of consolidating the agency-based data centers into the enterprise data center model. As of November 2016, MN.IT had reduced the total number of data centers from 49 to 28.

Objectives, Scope, and Methodology

Our audit examined the department's information technology controls in place, as of November 2016, to protect the facilities and the computing equipment contained in them.

Our audit focused on answering the following questions:

- Did the Office of MN.IT Services have adequate controls to provide reasonable assurance that it:
  - Protected the physical access to its data centers and their operating environments?
  - Protected electronic data being backed up and retained in its data centers?
  - Could recover operations of the data centers in the event of a disaster?
  - Could respond to an incident affecting the operations of its data centers?[6]
- Did the Office of MN.IT Services comply with state and federal legal requirements and the MN.IT policies and procedures we tested?

To meet the above objectives, we interviewed MN.IT management and staff to gain an understanding of the MN.IT data center information technology policies and procedures. We examined the controls at the two enterprise data centers, as well as at two agency-based data centers we selected for testing. We considered the risk of potential weaknesses surrounding the data centers' computer systems and noncompliance with relevant legal requirements.

We reviewed the controls as of November 2016 in the following information technology areas:

[6] A data center incident is an unplanned event that is not part of normal operations that disrupts operational processes, such as an equipment failure or a power outage. A configuration change is a planned event to install, move, or replace equipment or components within the data center.

- For its enterprise data centers and agency-based data centers, we reviewed who had physical access to the centers and observed the equipment to ensure that MN.IT adequately:
  - Regulated the air temperature;
  - Monitored for smoke, fire, and water;
  - Monitored and protected the continuity of the power supply, including backup power; and
  - Restricted access.
- For its enterprise data centers, we examined the controls over MN.IT's computer systems to detect processing errors or data center configuration changes. We:
  - Reviewed the process for recording and resolving operations incidents;
  - Reviewed the process for requesting, recording, and implementing changes to data center equipment;
  - Tested a sample of data center incidents to ensure that staff properly responded to and resolved incidents in accordance with MN.IT policies; and
  - Tested a sample of data center configuration changes to ensure that MN.IT staff properly resolve the changes we tested in accordance with MN.IT policies.
- We examined the controls over data backup and the ability to restore data if a problem occurred at a data center. We:
  - Reviewed contingency planning documentation; and
  - Reviewed processes for backing up and storing system data.

Our audit did not examine controls related to the specific software operating in MN.IT data centers for any specific agencies.

We conducted the audit in accordance with generally accepted government auditing standards.[7] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

We assessed MN.IT's controls against MN.IT's standards, policies, and procedures and against the information technology standards of the *National Institute of Standards and Technology Special Publication 800-53 (Revision 4)*

[7] U.S. Government Accountability Office, *Government Auditing Standards*, December 2011.

Security and Privacy Controls for Federal Information Systems and Organizations, published by the U.S. Department of Commerce in April 2013.[8]

Conclusion

The Office of MN.IT Services had generally adequate information technology controls to provide reasonable assurance that it protected the physical access and operational environment of the computer equipment, networking systems, and components in its enterprise data centers and the agency-based data centers we tested. The Office of MN.IT Services also generally complied with related applicable state and federal legal requirements and MN.IT policies and procedures we tested.

However, the Office of MN.IT Services had some weaknesses related to the operation of agency-based data centers and the updating, testing, and training for the disaster recovery plan for the enterprise data centers.

The following *Findings and Recommendations* section provides further explanation about the exceptions noted above.

[8] The *National Institute of Standards and Technology Special Publication 800-53* provides information technology standards for the federal government. These standards are widely accepted security standards and guidelines and are not only used by the federal government, but are frequently adopted on a voluntary basis by many organizations in the private sector.

Findings and Recommendations

Finding 1

The Office of MN.IT Services did not have adequate physical or environmental controls for some of the agency-based data centers it operates.

Good computer controls require that data centers implement strong physical controls and environmental safeguards to help ensure continuous availability of computer systems and protect the computer systems and data.[9]

The majority of the data centers that state agencies use are agency-based data centers and primarily serve the computing needs of an individual agency. As part of its information technology consolidation efforts, MN.IT has been working towards consolidating the computer operations for all state agencies into an enterprise data center model, which will serve multiple agencies. The enterprise data center model also includes duplication of physical and environmental controls beyond those typically found in agency-based data centers, including multiple power system supplies to the data centers and systems for continuous monitoring and logging of data center activity.

We reviewed the physical and environmental controls at four data centers MN.IT operates – two enterprise data centers and two agency-based data centers. The enterprise data centers house the computer equipment and support the systems used by multiple agencies, while the agency-based data centers primarily house the equipment and systems used by a single agency.

The two agency-based data centers we tested had the following weaknesses in their physical and environmental controls:

- One of the agency-based data centers did not adequately limit physical access. Non-MN.IT and non-agency staff had physical access to the data center. The data center is in a building leased by the state, and custodial and maintenance staff employed by the building's owner have access to the data center. Because the computer system in this data center did not encrypt the agency data and stored data on tapes, anyone with access to the data center had access to the data.
- One of the agency-based data centers also did not have a water detection system that would alert MN.IT to water in the data center.

[9] April 2013, National Institute of Standards and Technology Special Publication 800-53 (Revision 4) *Security and Privacy Controls for Federal Information Systems and Organizations*, PE-2, Physical Access Authorizations; PE-3, Physical Access Control; PE-6, Monitoring Physical Access; PE-8, Visitor Access Records; PE-9, Power Equipment and Cabling; PE-13, Fire Protection; PE-14, Temperature and Humidity Controls; PE-15, Water Damage Protection; PE-18, Location of Information Systems Components.

- One of the agency-based data centers did not have a raised floor, resulting in the computer equipment being stored in racks on the floor of the data center; this increases the risk of damage to the equipment in the event of water entering the data center.
- Neither of the agency-based data centers had duplicate power feeds from the public utility.

The control weaknesses we found at the agency-based data centers we reviewed indicate potential risks that may exist at the other 26 agency-based data centers. For example, several agency-based data centers have suffered power outages over the past year that have caused interruption to the computer processing for their respective agencies; in some cases, these power outages resulted in employees being unable to perform their job duties until power could be restored to the facilities. Consolidation of these agency-based data centers into the enterprise data centers would provide better assurance of adequate physical and environmental controls.

Recommendation

- *The Office of MN.IT Services should continue to consolidate the remaining agency-based data centers into the enterprise data center model.*

Finding 2

The Office of MN.IT Services did not update or test the contingency plan for the enterprise data centers in a timely manner.

Good information technology controls require that an organization develop and document a formal disaster recovery plan to assist the organization in recovering its critical information technology operations in a timely manner. The contingency plan is necessary to guide an organization in its response to an adverse or disaster event in the data center, such as:

- Flood or fire;
- Loss of power;
- Security breach; or
- Weather-related event, such as a tornado.

In addition to developing a plan, good controls require the organization to periodically update and test the plan and to train employees on how to implement it.[10] MN.IT has incorporated these disaster recovery plan expectations into its standards.[11] MN.IT standards require MN.IT, on an annual basis, to update and test the plan and train staff in how to execute the plan.

However, as of November 2016, MN.IT had not updated its disaster recovery plan since 2014 and had not tested the plan since 2012. In addition, MN.IT had not conducted formal training for individuals responsible for executing the disaster recovery plan.

Recommendation

- *MN.IT should update, test, and provide training on its disaster recovery plan for the enterprise data centers at least annually.*

[10] April 2013, National Institute of Standards and Technology Special Publication 800-53 (Revision 4) *Security and Privacy Controls for Federal Information Systems and Organizations*, CP-2, Contingency Plan; CP-3, Contingency Training; CP-4, Contingency Plan Testing; CP-7, Alternate Processing Site; CP-9, Information System Backup.

[11] MN.IT Enterprise Contingency Planning Standard.


THE GREAT SEAL OF THE STATE OF MINNESOTA
L'ETOILE DU NORD
1858

February 28, 2017

Mr. James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street Suite 140
St. Paul, Minnesota 55155

Dear Mr. Nobles,

I would like to begin by thanking your team for the work done on this audit of MN.IT Data Center Controls. Your team was courteous, highly professional, and took the time to listen as we explained the difference between the enterprise datacenter model and the standalone agency datacenter model, which predated Minnesota IT Services.

The enterprise datacenter model has substantially better physical, environmental, and cybersecurity controls. This is why Minnesota IT Services has been striving to migrate agency technology operations to enterprise datacenters. I am pleased to report that we reduced the number of standalone agency datacenters from 49 to 27 since the 2011 IT consolidation legislation. These efforts have taken advantage of one-time agency contributions, often during times when standalone agency datacenters experienced serious outages or needed major repairs.

We appreciate this audit because it demonstrates the stark difference between the old and new datacenter management models. The findings also underscore the urgency of our budget request currently before the Legislature to accelerate the pace of migrations to highly secure enterprise datacenters.

Thank you once again for the outstanding work on this extremely important topic. Nothing is more important to Minnesota IT Services than protecting the security of data and ensuring the ongoing availability of critical government services.

Sincerely,

Thomas Baden, Commissioner
Minnesota IT Services

Finding 1. The Office of MN.IT Services does not have adequate physical or environmental controls for some of the agency-based datacenters it operates.

Minnesota IT Services agrees with this finding and has been actively working on implementing the recommendation since the IT consolidation legislation passed in 2011.

As this audit shows, enterprise datacenters have more robust physical, environmental and cybersecurity controls. Over the past six years, Minnesota IT Services has reduced the number of standalone agency datacenters from 49 to 27. However, Minnesota IT Services is not satisfied with this pace and is seeking resources to expedite the remaining migrations.

Minnesota IT Service's current legislative request includes approximately $14.1 million to build out the technology infrastructure of the existing enterprise datacenters. This one-time request also includes some funding for professional migration services. With a one-time appropriation, Minnesota IT Services expects to have all agency-based technology environments migrated to enterprise datacenters within 2 years. Absent funding, the current opportunistic approach will result in a 5 to 6 year migration timeline.

Person Responsible: Thomas A. Schaeffer, Assistant Commissioner of Enterprise Services

Anticipated Resolution Date: July 1, 2019 to July 1, 2023, depending on resource availability

Finding 2. The Office of MN.IT Services did not update or test the contingency plan for the enterprise data centers in a timely manner

Minnesota IT Services agrees with this finding and hopes to build a team to develop and test disaster recovery strategies for the enterprise datacenters and other major state computer systems.

Several years ago Minnesota IT Service's General Fund appropriation was reduced substantially. This budget reduction eliminated all funding for our central disaster recovery team. Minnesota IT Services transferred the salary of one team member to rate-based services. However, due to customer pushback we were not able to retain the four remaining staff.

Minnesota IT Service's current legislative request includes $600,000 to reconstitute a central disaster recovery planning team. This team will develop and test recovery strategies for the enterprise datacenters and other major systems across state government. Absent funding, Minnesota IT Services will continue looking for ways to repurpose IT consolidation savings to slowly rebuild a disaster recovery planning team.

Person Responsible: Jesse Oman, Deputy Commissioner

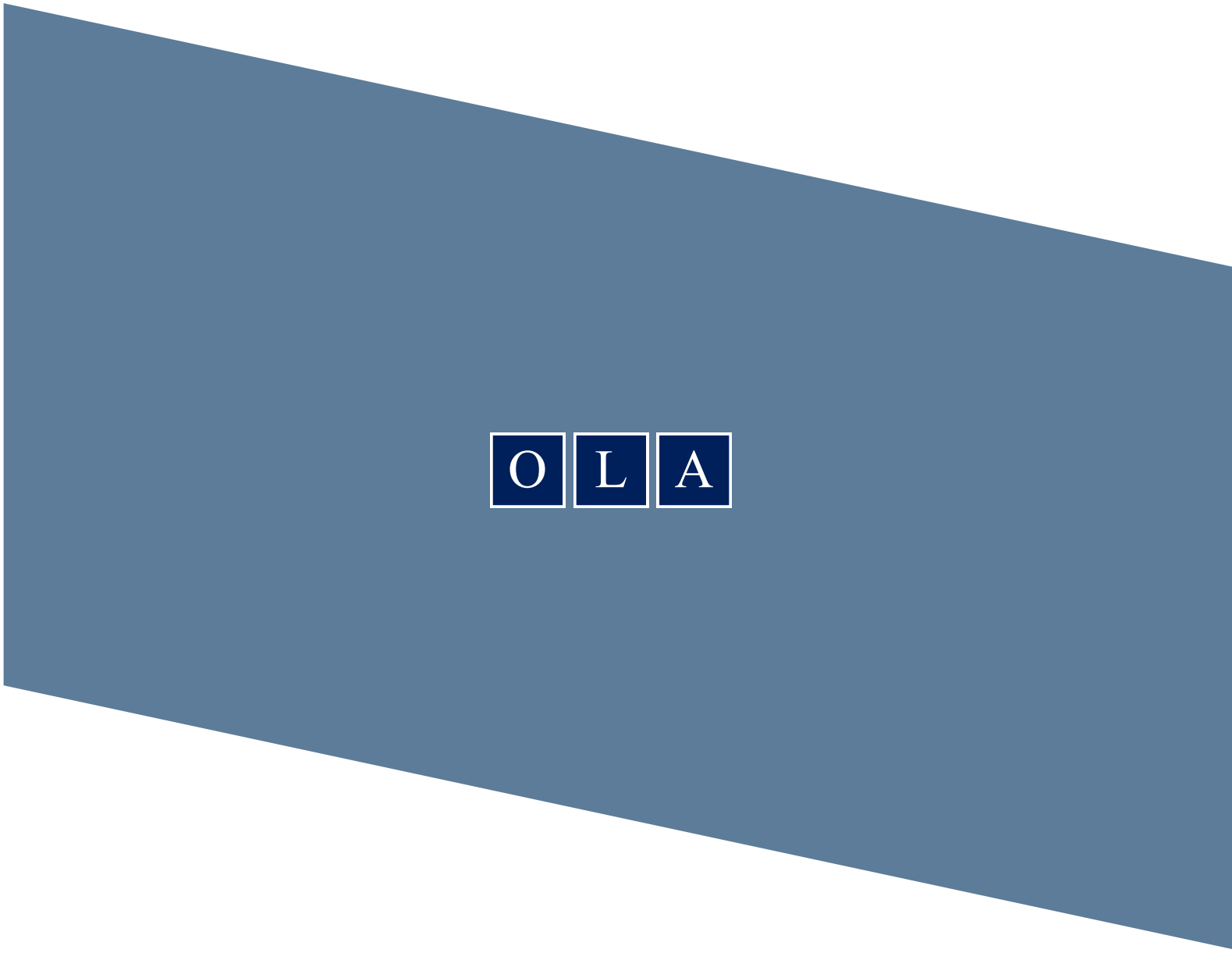
Anticipated Resolution Date: July 1, 2018 to July 1, 2020, depending on resource availability

For more information about OLA and to access its reports, go to: www.auditor.leg.state.mn.us.

To offer comments about our work or suggest an audit, evaluation, or special review, call 651-296-4708 or email legislative.auditor@state.mn.us.

To obtain printed copies of our reports or to obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

Printed on Recycled Paper



OFFICE OF THE LEGISLATIVE AUDITOR
CENTENNIAL OFFICE BUILDING – SUITE 140
658 CEDAR STREET – SAINT PAUL, MN 55155