MICHIGAN

OFFICE OF THE AUDITOR GENERAL

# AUDIT REPORT

PERFORMANCE AUDIT
OF THE

## CENTRALIZED INFORMATION TECHNOLOGY BACKUP SERVICE

DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

November 2012

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

071-0511-12

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

– Article IV, Section 53 of the Michigan Constitution

Audit report information can be accessed at:
*http://audgen.michigan.gov*

Michigan

*Office of the Auditor General*

# REPORT SUMMARY

## *Performance Audit*
## *Centralized Information Technology Backup Service*
## *Department of Technology, Management, and Budget*

**Report Number:**
**071-0511-12**

**Released:**
**November 2012**

*A backup is a copy of one or more data files created in case the original data file becomes lost or unusable. Regularly backing up data is one of the most effective ways to mitigate service interruptions. The Enterprise Backup and Recovery Group (EBUR), Department of Technology, Management, and Budget (DTMB), is responsible for the backup and restore of approximately 2,000 servers located in three DTMB hosting centers. In fiscal year 2010-11, EBUR billed State agencies $8.9 million for backup and recovery services.*

***Audit Objective:***
To assess the effectiveness of DTMB's efforts to back up data and system files for the State's critical applications in accordance with agency specifications or DTMB's default backup standard.

***Audit Conclusion:***
DTMB's efforts to back up data and system files for the State's critical applications in accordance with agency specifications or DTMB's default backup standard were moderately effective. We noted one reportable condition (Finding 1).

***Reportable Condition:***
DTMB had not fully established effective service level agreements (SLAs) relating to backup and recovery services for the State's critical applications (Finding 1).

***Noteworthy Accomplishments:***
DTMB won the 2008 National Association of State Chief Information Officers Award for Business Continuity and Disaster Recovery for its implementation of an enterprise storage and backup and recovery environment. DTMB also won a 2009 Best Practices in Storage award from Storage Networking World, in conjunction with Computerworld and the Storage Networking Industry Association, in the category of Storage Reliability and Data Recovery.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

***Audit Objective:***
To assess the effectiveness of DTMB's efforts to verify the integrity of backup data and system files for the State's critical applications.

***Audit Conclusion:***
DTMB's efforts to verify the integrity of backup data and system files for the State's critical applications were effective. Our audit report does not include any reportable conditions related to this audit objective.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

***Audit Objective:***
To assess the effectiveness of DTMB's efforts to secure the State's centralized backup data and system files.

***Audit Conclusion:***
DTMB's efforts to secure the State's centralized backup data and system files were moderately effective. We noted two reportable conditions (Findings 2 and 3).

***Reportable Conditions:***
DTMB did not encrypt sensitive and confidential data on the centralized backup files for the State's critical applications (Finding 2).

DTMB had not fully established effective security and access controls for the operating system of the EBUR media servers (Finding 3).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

***Agency Response:***
Our audit report contains 3 findings and 3 corresponding recommendations. DTMB's agency preliminary response indicates that it agrees with all 3 recommendations and has complied or will comply with them.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

**Thomas H. McTavish, C.P.A.**
Auditor General

**Scott M. Strong, C.P.A., C.I.A.**
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

November 14, 2012

John E. Nixon, C.P.A., Director
Department of Technology, Management, and Budget
George W. Romney Building
Lansing, Michigan
and
Mr. David B. Behen, Chief Information Officer
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Nixon and Mr. Behen:

This is our report on the performance audit of the Centralized Information Technology Backup Service, Department of Technology, Management, and Budget.

This report contains our report summary; description of agency; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's response subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Thomas H. McTavish, C.P.A.
Auditor General

This Page Left Intentionally Blank

# TABLE OF CONTENTS

## CENTRALIZED INFORMATION TECHNOLOGY BACKUP SERVICE
## DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

Backup Service

A backup is a copy of one or more data files created in case the original data file becomes lost or unusable. Regularly backing up data is considered to be one of the most cost-effective ways to mitigate service interruptions. It is important for an entity to be able to restore data. Without backup files, it may be impossible to re-create and restore data. For government agencies, some legal and financial regulations contain specific backup requirements.

The State of Michigan has implemented a centralized backup and recovery service within the Department of Technology, Management, and Budget (DTMB), which is provided as an option to executive branch departments and agencies.

Technical Services Division, Enterprise Backup and Recovery Group (EBUR)

DTMB's Technical Services Division is responsible for supporting and maintaining the infrastructure of the State's most critical servers.

EBUR is 1 of 5 groups within the Technical Services Division. EBUR is responsible for the centralized backup and restore of approximately 2,000 servers located in three DTMB hosting centers. Approximately 600 other servers are not backed up or restored by EBUR for various reasons, such as the server is vendor supported or no data resides on the server. EBUR consists of both State employees and contractors from Oracle Corporation (formerly Sun Microsystems). EBUR performs the backup of data on a regular basis within a scheduled time frame and performs data restores upon agency request. EBUR uses the NetBackup software and Microsoft Data Protection Manager (DPM) to coordinate backups at the three DTMB hosting centers. The backups are performed such that all data from the Secondary Complex hosting centers is stored downtown, while all of the data from downtown is stored at the Secondary Complex.

EBUR is responsible for providing backup services for approximately 600 servers associated with 68 critical State applications. These critical applications help State departments deliver important government services, such as:

- Processing services for and payments to the State's needy citizens.
- Managing prisoner, parolee, and probationer information.

- Maintaining voter registration.
- Processing the State employee payroll.
- Managing the State Employees' Retirement System.

EBUR charges State agencies a rate of $0.34 per gigabyte per month for backup and recovery services. In fiscal year 2010-11, EBUR billed State agencies $8.9 million through interagency transfers for backup and recovery services.

## Audit Objectives, Scope, and Methodology and Agency Responses

### Audit Objectives

Our performance audit* of the Centralized Information Technology Backup Service, Department of Technology, Management, and Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of DTMB's efforts to back up data and system files for the State's critical applications in accordance with agency specifications or DTMB's default backup standard.

2. To assess the effectiveness of DTMB's efforts to verify the integrity of backup data and system files for the State's critical applications.

3. To assess the effectiveness of DTMB's efforts to secure the State's centralized backup data and system files.

### Audit Scope

Our audit scope was to examine the information processing and other records related to the centralized information technology backup service. We limited our review of backup and recovery to servers associated with critical applications located in the three DTMB hosting centers. Our review did not include servers associated with critical applications that are vendor hosted or critical applications that reside on mainframe computers. We conducted this performance audit in accordance with generally accepted government auditing standards. 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 believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our audit procedures, conducted from June through August 2012, generally covered the period October 2011 through July 2012.

** See glossary at end of report for definition.*

Audit Methodology

We conducted a preliminary review of the centralized information technology backup service to establish our audit objectives. We obtained an understanding of DTMB's process to back up data and system files. We used the results of our preliminary review to determine the extent of our detailed analysis and testing.

To accomplish our first objective, we reviewed the listing of the 68 most critical applications to State government as identified by DTMB. We selected a random sample of 23 critical applications and performed testing to verify that backups of the State's critical applications were being performed according to agency specifications or the DTMB default backup standard. We also performed testing to verify that the State's critical applications were listed in service level agreements between State agencies and DTMB. We reviewed the service level agreements to determine whether the responsibility, expectations, and needs of the agencies were clearly communicated in the documents.

To accomplish our second objective, we interviewed DTMB staff to gain an understanding of the backup restore testing process. We verified that DTMB performed backup restore tests for the State's critical applications. Also, we surveyed State agencies regarding DTMB's ability to restore data as requested.

To accomplish our third objective, we interviewed DTMB staff to gain an understanding of the security* of the operating system* servers used to back up data. We tested the security of a sample of media servers* used in the backup process to verify that they were secured according to Center for Internet Security* benchmarks. Also, we reviewed the security of the hosting centers where the servers and backup tapes are located.

When selecting activities or programs for audit, we use an approach based on assessment of risk and opportunity for improvement. Accordingly, we focus our audit efforts on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. Our limited audit resources are used, by design, to identify where and how improvements can be made. Consequently, we

** See glossary at end of report for definition.*

prepare our performance audit reports on an exception basis. To the extent practical, we add balance to our audit reports by presenting noteworthy accomplishments for exemplary achievements identified during our audits.

Agency Responses

Our audit report contains 3 findings and 3 corresponding recommendations. DTMB's agency preliminary response indicates that it agrees with all 3 recommendations and has complied or will comply with them.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require DTMB to develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

# COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

# EFFECTIVENESS OF EFFORTS TO BACK UP DATA AND SYSTEM FILES

## COMMENT

**Audit Objective:** To assess the effectiveness of the Department of Technology, Management, and Budget's (DTMB's) efforts to back up data and system files for the State's critical applications in accordance with agency specifications or DTMB's default backup standard.

**Audit Conclusion: DTMB's efforts to back up data and system files for the State's critical applications in accordance with agency specifications or DTMB's default backup standard were moderately effective.** Our assessment disclosed one reportable condition* related to service level agreements (Finding 1).

**Noteworthy Accomplishments:** DTMB won the 2008 National Association of State Chief Information Officers Award for Business Continuity and Disaster Recovery for its implementation of an enterprise storage and backup and recovery environment. DTMB also won a 2009 Best Practices in Storage award from Storage Networking World, in conjunction with Computerworld and the Storage Networking Industry Association, in the category of Storage Reliability and Data Recovery.

## FINDING

1. Service Level Agreements

   DTMB had not fully established effective service level agreements (SLAs) relating to backup and recovery services for the State's critical applications. As a result, misunderstandings could occur between DTMB and the various State departments regarding the backup and recovery services provided by DTMB.

   Executive Order No. 2009-55 requires that DTMB develop SLAs with executive branch departments and agencies to ensure that quality information technology* services are delivered. According to Control Objectives for Information Related Technology* (COBIT), the purpose of an SLA is to establish the roles, responsibilities, and performance expectations for information technology services that are provided. An effective SLA should include such items as the identification

** See glossary at end of report for definition.*

of critical applications, frequency of backup performance, retention period of backup data, and frequency for testing the integrity of the backup files.

We reviewed 10 SLAs between DTMB and various State departments covering 55 critical applications. Our review disclosed:

a. The SLAs for all 10 of the departments did not describe the frequency of backups, retention period of backup data, and frequency for testing the integrity of the backup files.

b. The SLAs for the Departments of Community Health, Corrections, Human Services, Licensing and Regulatory Affairs, State, and Education did not include 14 (25%) of the 55 critical applications owned by those departments. For example, the backup and recovery services for the following critical applications were not included in an SLA:

- Community Health Automated Medicaid Processing System (CHAMPS)
- Sales, Inventory, and Purchasing System (SIPS)
- Unemployment Compensation Claims Processing
- Business Application Modernization (BAM) on-line services

## RECOMMENDATION

We recommend that DTMB fully establish effective SLAs relating to backup and recovery services for the State's critical applications.

## AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it has already taken steps to comply with the recommendation. DTMB's Enterprise Backup and Recovery Group (EBUR) and Enterprise Storage Group informed us that DTMB contracted with a third party service provider in June 2012 to improve the organization's SLA and operational level agreement processes. As a result, the Technical Service Division is in the process of updating DTMB's Service Catalog, based on industry best practices, to improve DTMB's service communication with customers. Once completed, the Technical Services Division will review all current SLAs and will generate recommendations to incorporate backup and recovery service information into all SLAs. DTMB informed us that recommendations will be completed by November 15, 2012, with implementation completed by November 30, 2012.

## EFFECTIVENESS OF EFFORTS TO VERIFY THE INTEGRITY OF BACKUP DATA AND SYSTEM FILES

### COMMENT

**Background:** In 2010, DTMB began an initiative to test backup files to ensure that the data on those files could be restored. DTMB selected servers that support the State's critical applications upon which to perform the restore tests. As of July 2012, DTMB had performed restore tests of backup data for 381 (65%) of 582 servers that are associated with 68 of the State's critical applications. DTMB plans to complete testing on the 582 servers and will then establish a schedule for regular backup restore testing.

**Audit Objective:** To assess the effectiveness of DTMB's efforts to verify the integrity of backup data and system files for the State's critical applications.

**Audit Conclusion: DTMB's efforts to verify the integrity of backup data and system files for the State's critical applications were effective.** Our audit report does not include any reportable conditions related to this audit objective.

## EFFECTIVENESS OF EFFORTS TO SECURE THE STATE'S CENTRALIZED BACKUP DATA AND SYSTEM FILES

### COMMENT

**Audit Objective:** To assess the effectiveness of DTMB's efforts to secure the State's centralized backup data and system files.

**Audit Conclusion: DTMB's efforts to secure the State's centralized backup data and system files were moderately effective.** Our assessment disclosed two reportable conditions related to encryption and operating system security and access controls* (Findings 2 and 3).

** See glossary at end of report for definition.*

## FINDING

2. Encryption

DTMB did not encrypt sensitive and confidential data on the centralized backup files for the State's critical applications. As a result, DTMB cannot ensure that sensitive and confidential data is protected from unauthorized disclosure.

Encryption is the conversion of data into an unreadable format. DTMB Technical Standard 1340.00.07 requires the use of encryption when data is transmitted or when data is stored in permanent or removable electronic media to minimize the likelihood that sensitive or confidential data will be inadvertently disclosed or accessed.

DTMB performs backups of servers associated with 68 of the State's critical applications. Fifty (74%) of the 68 critical applications backed up by DTMB contain sensitive and confidential data that should be secured from unauthorized disclosure, such as birth dates, addresses, and healthcare records. However, DTMB did not encrypt the backup data for any of these critical applications.

In October 2011, EBUR selected a software solution that will allow it to encrypt data written to physical tape storage using the Oracle Key Manager software. DTMB informed us that it completed the implementation of the solution in September 2012.

## RECOMMENDATION

We recommend that DTMB encrypt sensitive and confidential data on the centralized backup files for the State's critical applications.

## AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it has already taken steps to comply with the recommendation. DTMB informed us that it has completed the implementation of physical tape hardware encryption within the backup and recovery environment. To ensure that encryption compliance is covered within the backup and recovery environment, EBUR informed us that it has defined a standard to determine which server backups require encryption. EBUR also informed us that it has begun a project to migrate these backups to physical tape encrypted storage. In addition, DTMB informed us that encryption of all Red Card application backups will be completed by December 31, 2012.

## FINDING

3. Operating System Security and Access Controls

DTMB had not fully established effective security and access controls for the operating system of EBUR media servers. As a result, DTMB cannot ensure that centralized backup data is protected from unauthorized modification, loss, or disclosure.

DTMB Technical Standard 1340.00.03 requires the secure establishment, maintenance, and administration of servers, including the operating system and data residing on the servers. To achieve a secure operating system, the standard requires that controls be established to protect information and resources from unauthorized access. In addition, it requires that the operating system be installed with a minimal service configuration to reduce the risk of network intrusion or the exploitation of well-known operating system vulnerabilities*.

We sampled 15 (71%) of the 21 media servers used in the backup and recovery process. We identified potentially vulnerable operating system configurations, according to the Center for Internet Security benchmarks, on 9 (60%) of the 15 servers. Because of the confidentiality of operating system configurations, we summarized the results of our testing for presentation in this finding and provided the detailed results to DTMB.

## RECOMMENDATION

We recommend that DTMB fully establish effective security and access controls for the operating system of EBUR media servers.

## AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it has already taken steps to comply with the recommendation. EBUR informed us that it has implemented a new process to regularly notify and assign staff members a task to review and validate all user accounts on EBUR servers and devices in order to ensure that invalid user accounts are removed. EBUR also informed us that it initiated a project in January 2012 to refresh all backup media servers with automated tools in order to reduce the vulnerability footprint and increase the security posture of servers within the

** See glossary at end of report for definition.*

backup and recovery environment. In addition, DTMB informed us that, as of September 2012, the automated tools have been installed and more than 50% of network backups have been migrated to this new infrastructure. Full migration of all network backups to the automated tool will be completed by March 31, 2013.

# GLOSSARY

## Glossary of Acronyms and Terms

| | |
|---|---|
| access controls | Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts. |
| Center for Internet Security | A not-for-profit organization that establishes and promotes the use of consensus-based best practice standards to raise the level of security and privacy in information technology systems. |
| Control Objectives for Information and Related Technology (COBIT) | A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over information technology. |
| DTMB | Department of Technology, Management, and Budget. |
| EBUR | Enterprise Backup and Recovery Group. |
| effectiveness | Success in achieving mission and goals. |
| information technology (IT) | Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources. |
| master server | A server that provides administration and control for backups and restores for all clients and servers in a master and media server cluster. |

| | |
|---|---|
| media server | A server that provides storage within a master and media server cluster. The master can also be a media server. |
| operating system | The essential program in a computer that manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer. |
| performance audit | An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability. |
| reportable condition | A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely or have occurred. |
| security | Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity. |
| SLA | service level agreement. |
| vulnerability | Weakness in an information system that could be exploited or triggered by a threat. |

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL