MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

STATEWIDE UNIX SECURITY

DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET

April 2010

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

084-0563-09

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

Statewide UNIX Security

Department of Technology, Management and Budget (DTMB)

Report Number:
084-0563-09

Released:
April 2010

DTMB maintains and operates approximately 550 servers with a UNIX operating system. These servers contain critical systems and data for the 15 State departments. These systems help the State departments deliver important government services. DTMB is responsible for the configuration, administration, and security of the UNIX servers. In 2009, at least $5 billion of transactions were processed by State departments on UNIX servers.

Audit Objective:
To assess the effectiveness of DTMB's controls to ensure the security of the State's UNIX servers.

Audit Conclusion:
DTMB's controls to ensure the security of the State's UNIX servers were moderately effective. We noted five reportable conditions (Findings 1 through 5).

Reportable Conditions:
DTMB did not fully develop an effective method to detect operating system weaknesses on UNIX servers (Finding 1).

DTMB did not fully remediate operating system security weaknesses on its UNIX servers (Finding 2).

DTMB should improve the accuracy and completeness of information in its UNIX server inventory (Finding 3).

DTMB had not fully established an appropriate segregation of duties over the administration of all UNIX servers (Finding 4).

DTMB did not fully establish procedures for the secure configuration of UNIX servers (Finding 5).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 5 findings and 5 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all of the recommendations and 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

April 13, 2010

Mr. Kenneth D. Theis, Director
Department of Technology, Management and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Theis:

This is our report on the performance audit of Statewide UNIX Security, Department of Technology, Management and Budget. This report contains our report summary; description of agency; audit objective, scope, and methodology and agency responses; comment, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

The agency preliminary responses were taken from the agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

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

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

STATEWIDE UNIX SECURITY
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET

Page

INTRODUCTION

COMMENT, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Agency

Executive Order 2009-55, effective March 21, 2010, abolished the Michigan Department of Information Technology and renamed the Department of Management and Budget as the Department of Technology, Management and Budget (DTMB). DTMB maintains and operates approximately 550 servers with a UNIX operating system. These servers contain critical systems and data for the 15 State departments. These systems help the State departments deliver important government services, including:

- Processing income and business tax returns.
- Maintaining voter registration information.
- Processing the State employee payroll.
- Processing services and payments to the State's needy citizens.
- Tracking and managing road and bridge construction projects and payments.
- Maintaining prisoner, parolee, and probation information.

UNIX servers also provide a variety of enterprise-wide functions, such as web, file, and print services; e-mail; patch* management; and virus protection, as well as the software that stores, organizes, and provides access to systems. DTMB runs 16 variations of UNIX operating systems on the State's servers. DTMB's Technical Services Division and Office of Enterprise Security share the responsibility for server security*. In 2009, at least $5 billion of transactions were processed by State departments on UNIX servers.

Technical Services Division

The Technical Services Division is responsible for the configuration* and administration of the UNIX servers. The Technical Services Division coordinates with other divisions within DTMB, as well as other State agencies, for the development, implementation, and maintenance of information technology supporting State agency business functions.

Office of Enterprise Security

The Office of Enterprise Security is responsible for identifying, managing, and mitigating security risks* and vulnerabilities* within the State of Michigan government computing, communication, and technology resources. The Office of Enterprise Security is also responsible for disaster recovery planning, risk management, security awareness and training, assistance to State agencies with their security issues, and enforcement oversight of State security policies and procedures intended to maintain suitable enterprise-wide security.

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

Audit Objective, Scope, and Methodology
and Agency Responses

Audit Objective

The objective of our performance audit* of Statewide UNIX Security, Department of Technology, Management and Budget (DTMB), was to assess the effectiveness* of DTMB's controls to ensure the security of the State's UNIX servers.

Audit Scope

Our audit scope was to examine the information processing and other records related to the security of UNIX servers. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our audit procedures, conducted from May through September 2009, generally covered the period September 2008 through September 2009.

Audit Methodology

We conducted a preliminary review of DTMB's controls over UNIX operating system security. We reviewed and obtained an understanding of DTMB's policies, standards, and procedures for UNIX operating system security. We used the results of our preliminary review to determine the extent of our detailed analysis and testing.

To accomplish our audit objective, we performed an assessment of the configuration and security of UNIX servers. We reviewed and evaluated the DTMB-developed script* that obtained server configuration information to determine if the script identified UNIX security weaknesses. We also reviewed and assessed whether DTMB identified server configuration information for both State and vendor operated UNIX servers. In addition, we reviewed and assessed DTMB's process to secure those UNIX servers that have security weaknesses. Further, we reviewed and assessed DTMB's policies and procedures for configuring and securing UNIX servers.

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

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 prepare our performance audit reports on an exception basis.

Agency Response

Our audit report contains 5 findings and 5 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all of the recommendations and 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 formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENT, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF UNIX SECURITY

COMMENT

Background: In its October 2008 bulletin, the Information Technology Laboratory, National Institute of Standards and Technology* (NIST), explained that the first step in the security of an information system is securing its operating system. Securing the operating system is necessary because operating system manufacturers, who are unaware of each organization's unique security requirements, often configure their hardware and software to emphasize functionality and ease of use at the expense of security. The goal of effective security is to minimize to an acceptable level the risk of exposure to threats* that impact the confidentiality, integrity, and availability of data and information systems.

The Department of Technology, Management and Budget's (DTMB's) Technical Services Division began the implementation of a UNIX security remediation* project in September 2008. As part of that project, the Technical Services Division developed an automated program (script) to help identify up to 47 potential operating system weaknesses on the State's UNIX servers. Remediation of the identified weaknesses could help ensure that servers are configured securely according to industry best practices.

DTMB informed us that the State is compliant with Payment Card Industry (PCI) Security Standards. PCI compliance is achieved by implementing standards set by the PCI Security Standards Council for ensuring the security of credit card holder data. However, PCI compliance does not ensure that operating system vulnerabilities do not exist on a server. In addition, not all of the State's UNIX servers are scanned for the PCI Security Standards because some servers do not store, process, or transmit credit card holder data. As stated in NIST's Guide to General Server Security, it takes only one insecurely configured server to compromise a network.

Recent Office of the Auditor General information technology audits of systems at the former Department of Management and Budget, former Department of Civil Service, Department of Transportation, and Department of Corrections identified material conditions* or reportable conditions* related to the security of UNIX servers.

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

Audit Objective: To assess the effectiveness of DTMB's controls to ensure the security of the State's UNIX servers.

Audit Conclusion: DTMB's controls to ensure the security of the State's UNIX servers were moderately effective. Our assessment disclosed five reportable conditions related to detection of operating system weaknesses, remediation of UNIX servers, inventory of server information, segregation of duties*, and server configuration procedures (Findings 1 through 5).

FINDING

1. Detection of Operating System Weaknesses

DTMB did not fully develop an effective method to detect operating system weaknesses on UNIX servers. As a result, DTMB cannot ensure that data and information systems were protected from vulnerabilities that could threaten the security of the State's information systems and data.

NIST's Guide to General Server Security states that, to secure a server, it is essential to first identify the weaknesses that must be remediated. If a server has known vulnerabilities that attackers could exploit, the vulnerabilities should be removed or mitigated. DTMB scans 65 UNIX servers monthly for PCI compliance to identify certain UNIX operating system vulnerabilities. DTMB also developed a script to identify approximately 47 potential operating system weaknesses that need remediation. This script is based on a federal security checklist of UNIX weaknesses that categorizes vulnerabilities according to severity. Our review of DTMB's process to identify UNIX operating system weaknesses disclosed:

a. DTMB did not include in the script 16 (57%) of 28 Category 1 vulnerabilities in the federal security checklist. Category 1 vulnerabilities are severe weaknesses that could provide an attacker immediate system access, allow privileged user access, or bypass a firewall*.

b. DTMB did not include in the script 204 (85%) of 240 Category 2 vulnerabilities in the federal security checklist. Category 2 vulnerabilities are severe weaknesses that could provide an intruder with information needed to gain access to a system or a network.

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

c. DTMB's process to identify operating system weaknesses did not include analyzing all servers administered by DTMB. As a result, DTMB did not run its script on 135 (28%) of 489 servers. As a compensating control, DTMB scanned 81 of the 135 servers for PCI compliance at some time. However, it has never scanned 54 of the servers for PCI compliance. It is important to secure these servers because, for example, 5 of the State's critical business applications reside on 14 of these servers and 2 of these servers contain systems that, if not functioning, could affect the safety of State citizens.

d. DTMB did not periodically verify that vendors that administer UNIX servers follow the State's security standards. Vendor contracts require that vendors adhere to all of the State's existing technology standards. DTMB should obtain assurance of the vendor's compliance with the State's technology standards. We noted that one of the State's critical business applications runs on 15 servers administered by vendors.

RECOMMENDATION

We recommend that DTMB fully develop an effective method to detect operating system weaknesses on UNIX servers.

AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it is continuing to work on process improvements for UNIX system management. DTMB stated that it continues to advance internally developed solutions as well as explore open source and commercial solutions to UNIX system management and security.

FINDING

2. Remediation of UNIX Servers

DTMB did not fully remediate operating system security weaknesses on its UNIX servers. Remediation of operating system weaknesses will help reduce the risk of server or network intrusion and the exploitation of well-known operating system vulnerabilities.

NIST's Guide to General Server Security states that management should remediate known security weaknesses on a server to help prevent the exploitation of the weaknesses. DTMB used the script developed by the Technical Services

Division to identify operating system security weaknesses. We reviewed the script results and determined that DTMB remediated some UNIX operating system weaknesses. However, our review disclosed:

a. DTMB did not remediate all identified operating system weaknesses. Although 18 (5%) of 350 UNIX servers contained no identified operating system weaknesses, the following table illustrates the number of servers with unremediated weaknesses:

Number of Unremediated Operating System Weaknesses	Number of Servers
1 to 5	152 (43%)
6 to 10	82 (23%)
11 to 15	67 (19%)
16 to 20	24 (7%)
21 or more	7 (2%)

Examples of serious weaknesses that DTMB did not remediate include weak password and account lockout policies on 80 (23%) of 350 servers and removing or disabling unnecessary system accounts on 110 (31%) of 350 servers.

b. DTMB did not fully develop an effective process to track the remediation of all UNIX operating system security weaknesses. As a result, DTMB could not ensure that all server weaknesses were remediated or that the State agencies accepted the risk to their business functions. DTMB should require system administrators to record all remediation they have performed and identify weaknesses still in need of remediation. This would help ensure the correction of all security weaknesses.

RECOMMENDATION

We recommend that DTMB fully remediate operating system security weaknesses on its UNIX servers.

AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it is continuing to work on process improvements for UNIX system management. DTMB stated that it continues to advance internally developed solutions as well as explore open source and commercial solutions to UNIX system management and security.

FINDING

3. Inventory of Server Information

DTMB should improve the accuracy and completeness of information in its UNIX server inventory. Without an accurate and complete inventory, DTMB cannot effectively maintain and secure the State's UNIX servers.

NIST's Guide to General Server Security states that, in order to effectively secure operating system servers, an organization must identify its information technology assets, including hardware, software, system administrators, and system users. DTMB developed a configuration management database (CMDB) to record its inventory of UNIX servers. Our review of selected information contained in the CMDB disclosed:

a. DTMB did not ensure the accuracy of server information contained in the CMDB. We noted that DTMB recorded the wrong operating system for 15 servers, the wrong name for 6 servers, and the wrong system administrator for 3 servers. Also, DTMB incorrectly identified 3 decommissioned servers as operational and listed 2 servers twice in the CMDB. Without accurate server information in the CMDB, it could be difficult for DTMB to ensure that all UNIX servers are tested for security weaknesses.

b. DTMB did not ensure the completeness of server information in the CMDB. We identified instances of incomplete information in the CMDB, such as 57 UNIX servers that did not include the names of the application residing on the servers. In addition, we identified 3 servers that did not include the name of the operating system in the CMDB.

An accurate and complete inventory of UNIX server information is necessary to enable DTMB to identify and remediate all UNIX operating system weaknesses (Findings 1 and 2).

RECOMMENDATION

We recommend that DTMB improve the accuracy and completeness of information in its UNIX server inventory.

AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it will implement new quality assurance procedures to improve the accuracy of the CMDB. DTMB stated that it will publish a policy to require submission of a decommission request in Remedy when State servers are retired. DTMB also stated that it will initiate an Application Inventory Repository project to collect application data for all State servers. Once collected, the application portfolio will be managed from a single repository (CMDB). The CMDB will be modified to accommodate the new data. DTMB informed us that the project will identify and design processes necessary to maintain the data and educate DTMB staff about the process improvements.

FINDING

4. Segregation of Duties

DTMB had not fully established an appropriate segregation of duties over the administration of all UNIX servers. As a result, UNIX server administrators in the Agency Services Division could circumvent operating system controls that protect applications and data.

Control Objectives for Information and Related Technology* (COBIT) states that proper segregation of duties helps reduce the risk of an individual bypassing critical controls and inadvertent or intentional misuse of information. Segregation of duties would also help ensure the adequate oversight and secure configuration of UNIX servers.

DTMB assigned the role and responsibility of UNIX server administration to the Technical Services Division and assigned the role and responsibility of application and database administration to the Agency Services Division as a means to separate users with privileged access to servers from users with privileged access to applications and databases. However, we identified seven servers where an

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

Agency Services Division employee was the server administrator. DTMB should transfer these server administration functions and resources to the Technical Services Division to help reduce the risk of a single individual having the authority to bypass critical controls.

We reported the lack of segregation of duties in our performance audit of Network Application Server Controls (084-0555-05), issued in October 2006. The Michigan Department of Information Technology agreed with the recommendation and indicated that it would transfer server administration functions and resources managed by the Agency Services Division to the Technical Services Division by December 31, 2007.

RECOMMENDATION

We recommend that DTMB fully establish an appropriate segregation of duties over the administration of all UNIX servers.

AGENCY PRELIMINARY RESPONSE

DTMB agrees that segregation of duties is important and informed us that it has made great strides toward this goal with role changes and the use of the "sudo" utility. In addition, DTMB agrees that, of more than 500 servers, 7 still remain under the Agency Services Division's control. DTMB informed us that it will pursue transitioning these 7 servers.

FINDING

5. Server Configuration Procedures

DTMB did not fully establish procedures for the secure configuration of UNIX servers. As a result, DTMB cannot ensure that UNIX servers are secure and that responsibility for maintaining security is appropriately assigned.

DTMB should establish procedures to ensure that the operating system is installed with a minimal service configuration to reduce the risk of network intrusion and the exploitation of well-known operating system vulnerabilities. In addition, a well-secured operating system helps provide a stable platform on which to run application systems and other software.

a. DTMB did not establish and document procedures for the minimum operating system security configurations specific to UNIX servers. In addition, DTMB did not develop a policy requiring DTMB and State agencies to obtain an exemption from the minimum security configuration for applications with a valid reason for not complying with the standard security configurations. NIST's Guide to General Server Security states that organizations should develop standardized secure configurations to ensure system security.

b. DTMB did not establish procedures to require routine testing of UNIX security configurations. Periodic testing of operating system configurations would help detect UNIX operating system weaknesses for remediation.

c. DTMB did not develop procedures to require DTMB and State agencies to remediate identified UNIX operating system weaknesses, implement compensating controls, or document and accept the risk to the State's systems and data.

RECOMMENDATION

We recommend that DTMB fully establish procedures for the secure configuration of UNIX servers.

AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it has already completed work in this area and is continuing to implement process improvements related to UNIX system management and security.

GLOSSARY

Glossary of Acronyms and Terms

CMDB
configuration management database.

configuration
The way a system is set up. Configuration can refer to either hardware or software or the combination of both.

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.

effectiveness
Program success in achieving mission and goals.

firewall
Hardware and software components that protect one set of system resources (e.g., computers or networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.

material condition
A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.

National Institute of Standards and Technology (NIST)
An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.

patch

An update to an operating system, applications, or other software issued specifically to correct particular problems with the software.

PCI

Payment Card Industry.

performance audit

An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve program operations, to facilitate decision making by parties responsible for overseeing or initiating corrective action, and to improve public accountability.

remediation

The process to correct a fault or deficiency.

reportable condition

A matter that, in the auditor's judgment, 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 objectives of the audit; 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 to have occurred.

script

A list of commands that can be executed without user interaction.

security

Safeguarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

security risk

The probability that a particular security threat will exploit a system vulnerability.

segregation of duties

Separation of the management or execution of certain duties or areas of responsibility to prevent and reduce opportunities for unauthorized modification or misuse of data or service.

threat

An activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.

vulnerability

Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

STATE OF MICHIGAN

OFFICE of the AUDITOR GENERAL