

Office of the Auditor General

Performance Audit Report

Statewide UNIX Security Controls

Department of Technology, Management, and Budget

December 2015



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



OAG

Office of the Auditor General

Report Summary

Performance Audit

Statewide UNIX Security Controls

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0563-15

Released:
December 2015

DTMB maintains and operates approximately 950 UNIX servers. Systems and data critical for the operation of State government reside on these servers. The DTMB Technical Services Division is responsible for their configuration, administration, and security. The Cloud Automation and Audit Compliance teams provide oversight and support for UNIX security.

| Audit Objective | | | Conclusion |
|---|--------------------|----------------------|-----------------------------|
| Objective #1: To assess the effectiveness of DTMB's efforts to implement security and access controls over the State's UNIX servers. | | | Moderately effective |
| Findings Related to This Audit Objective | Material Condition | Reportable Condition | Agency Preliminary Response |
| DTMB did not establish and implement effective operating system security configuration controls for the State's UNIX server environment. We noted potentially vulnerable security configurations on 59 (94%) of 63 servers tested (Finding #1). | X | | Agrees |
| DTMB should establish a strategy to ensure that only supported UNIX operating system versions are installed on servers containing the State's applications. Unsupported versions were operational on approximately 30 of the State's UNIX servers, some of which contained systems considered critical to State government operations (Finding #2). | | X | Agrees |
| DTMB did not apply operating system patches in a timely manner for 90% of the servers tested. Patch management maintenance windows were not established for 559 (58%) of the State's UNIX servers (Finding #3). | | X | Agrees |
| DTMB did not establish and implement effective access controls over the State's UNIX operating systems to help prevent or detect inappropriate access to data (Finding #4). | | X | Agrees |

| Audit Objective | | | Conclusion |
|--|---------------------------|-----------------------------|------------------------------------|
| Objective #2: To assess the effectiveness of DTMB's efforts to establish an effective governance structure over the State's UNIX server environment. | | | Moderately effective |
| Findings Related to This Audit Objective | Material Condition | Reportable Condition | Agency Preliminary Response |
| DTMB did not fully establish and implement effective procedures to detect and remediate security vulnerabilities. Forty-seven percent of servers tested did not have a vulnerability scan in over one month. When performed at our request, the average number of high risk exposures detected on a server was 77 and the greatest number was 420 (<u>Finding #5</u>). | X | | Agrees |
| DTMB did not fully establish a segregation of duties over the administration of UNIX servers. The DTMB Agency Services Division had too much control over key processes, which increased the risk that controls designed to secure the State's information systems could be circumvented (<u>Finding #6</u>). | | X | Agrees |
| DTMB did not maintain an accurate record of UNIX server information, which is necessary to maintain server security and to ensure the ready availability of information for critical business decisions (<u>Finding #7</u>). | | X | Agrees |
| Observations Related to This Audit Objective | Material Condition | Reportable Condition | Agency Preliminary Response |
| DTMB contracted with a third party vendor in 2009 for administration of certain UNIX servers at an annual cost of approximately \$264,000. The contract required a transfer of knowledge to State employees. However, as of August 2015, the server administration functions were still performed by the vendor even though DTMB had 16 State employees capable of performing the functions (<u>Observation #1</u>). | Not applicable | Not applicable | Not applicable |

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

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

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General



OAG

Office of the Auditor General

201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • www.audgen.michigan.gov

Doug A. Ringler, CPA, CIA
Auditor General

December 17, 2015

Mr. David B. Behen
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. Behen:

I am pleased to provide this performance audit report on Statewide UNIX Security Controls, Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days of the date above 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,

Doug Ringler
Auditor General

TABLE OF CONTENTS

STATEWIDE UNIX SECURITY CONTROLS

| | <u>Page</u> |
|---|-------------|
| Report Summary | 1 |
| Report Letter | 3 |
| Audit Objectives, Conclusions, Findings, and Observations | |
| Implementing Security and Access Controls | 8 |
| Findings: | |
| 1. Improved security configuration controls needed to protect UNIX operating systems. | 10 |
| 2. Establishment of approved UNIX operating system versions needed to protect confidential and critical information. | 11 |
| 3. Improved patch management controls would help decrease the risk to the availability, confidentiality, and integrity of data. | 13 |
| 4. Improvements needed to UNIX operating system access controls. | 15 |
| Establishing Effective Governance Structure | 19 |
| Findings: | |
| 5. Enhancements to procedures for detecting and remediating security vulnerabilities are necessary. | 20 |
| 6. Segregation of duties could help ensure that critical operating system controls cannot be bypassed. | 25 |
| 7. Inventory management improvements needed to ensure timeliness of critical decisions. | 27 |
| Observations: | |
| 1. Transferring server administration to DTMB could result in cost savings. | 29 |
| Agency Description | 30 |
| Audit Scope, Methodology, and Other Information | 31 |
| Glossary of Abbreviations and Terms | 34 |

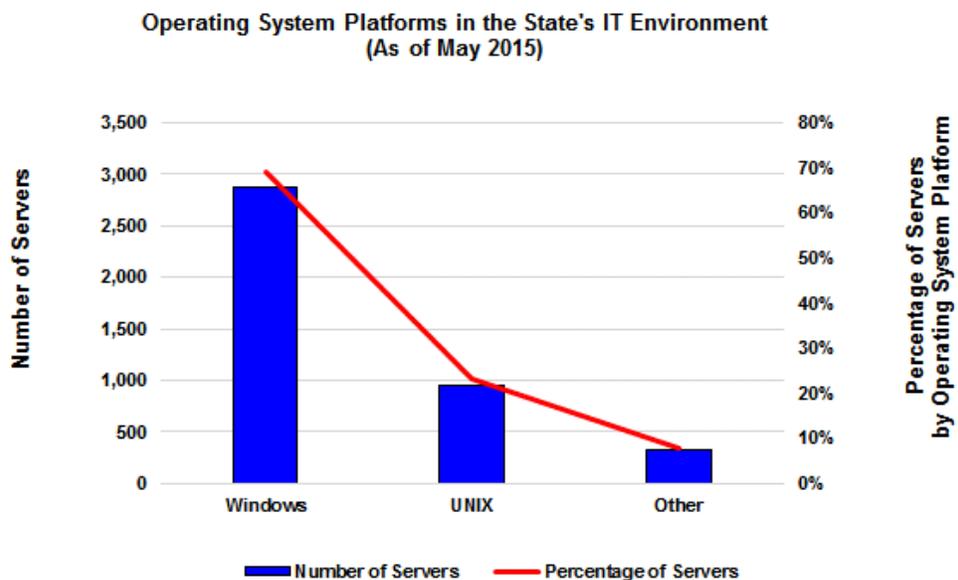
AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

IMPLEMENTING SECURITY AND ACCESS CONTROLS

BACKGROUND

A compromise of the operating system* exposes any application running on the system to vulnerabilities*. Lack of proper controls in an operating system may lead to attack or break-in from one system to another. Operating system security is composed of proper system configuration* and access controls.

The following chart depicts the number of servers by operating system platform and the percentage of the servers each operating system platform has in the State's information technology* (IT) environment:



AUDIT OBJECTIVE

To assess the effectiveness* of the Department of Technology, Management, and Budget's (DTMB's) efforts to implement security* and access controls* over the State's UNIX servers.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DTMB established some policies and procedures relating to UNIX security configurations and access controls.

* See glossary at end of report for definition.

- DTMB implemented some UNIX security configurations and access controls in accordance with DTMB policy and industry best practices.
- One material condition* (Finding #1) related to operating system security configuration controls.
- Three reportable conditions* (Findings #2 through #4) related to unsupported UNIX operating system versions, patch* management, and user access controls.

* See glossary at end of report for definition.

FINDING #1

Improvements to security configuration controls are needed to protect UNIX operating systems.

Potentially vulnerable security configurations found on 59 (94%) of 63 servers reviewed.

DTMB did not establish and implement effective operating system security configuration controls for the State's UNIX server environment. Ineffective configuration controls increase the risk of unauthorized access to the State's data and impairment to the integrity* and availability* of the State's critical information systems.

Well-secured operating systems help provide a stable and secure environment on which to run the State's applications. DTMB Administrative Guide policy 1340 requires the secure establishment, maintenance, and administration of servers, including the operating system software and the data residing on the servers. In addition, Control Objectives for Information and Related Technology* (COBIT) states that servers should be secured at a level equal to or greater than the defined requirements of the information being processed, stored, or transmitted.

We judgmentally selected 63 of the State's approximately 950 UNIX servers to review operating system security configurations. We noted potentially vulnerable security configurations on 59 (94%) of the 63 servers. We did not review the security configurations on the other 4 servers because they were running an unsupported operating system version (see Finding #2). Because of the confidentiality* of these configurations, we summarized our testing results for presentation in this finding and provided the detailed results to DTMB management.

As noted in Finding #5, DTMB did not fully establish and implement effective procedures to detect and remediate security vulnerabilities on the State's UNIX servers, which contributed to the weaknesses noted in this finding.

RECOMMENDATION

We recommend that DTMB establish and implement effective operating system security configuration controls for the State's UNIX server environment.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will improve operating system security configuration controls over the State's UNIX server environment. DTMB has purchased the necessary automation tools and has initiated a project to enforce and maintain effective standardized operating system security configuration controls.

* See glossary at end of report for definition.

FINDING #2

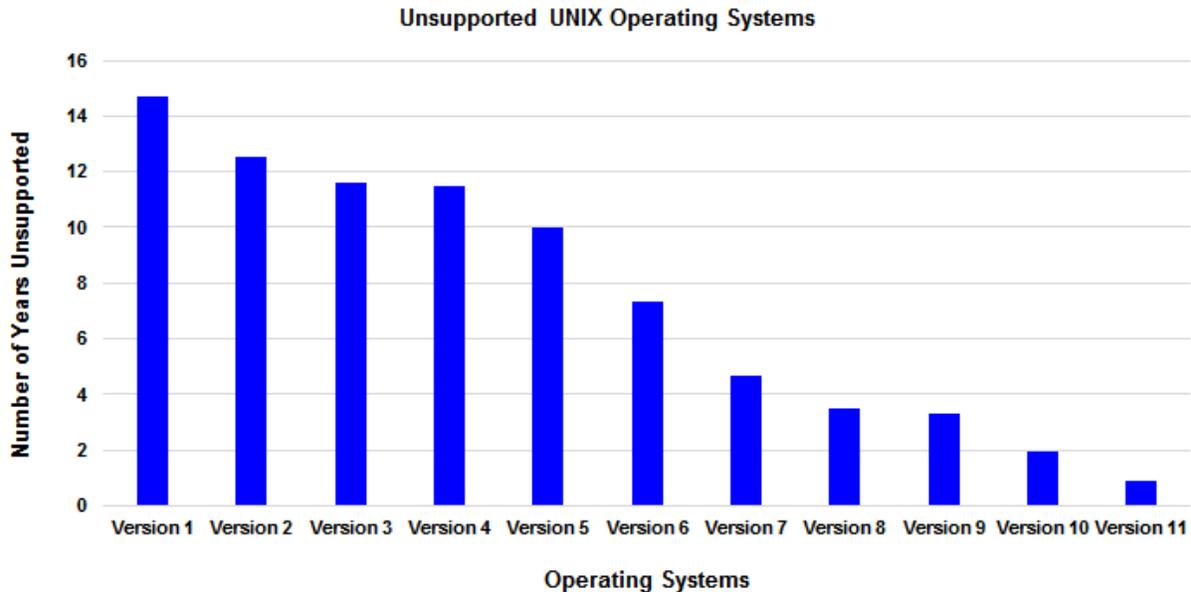
Establishment of approved UNIX operating system versions are needed to protect confidential and critical information residing on State systems.

Eleven unsupported UNIX operating system versions were identified on approximately 30 servers.

DTMB should establish a strategy to ensure that only supported UNIX operating system versions are installed on servers containing the State's applications. UNIX operating systems that are no longer supported by the vendor do not receive critical patches to address vulnerabilities, which increases the risk to availability, confidentiality, and integrity of data residing within the State's applications.

Executive Order No. 2009-55 charges DTMB with the responsibility of identifying standards and establishing controls to ensure that best practices are followed throughout the State's executive branch. Also, the National Institute of Standards and Technology* (NIST) states that upgrading the operating system to a supported version is essential to securing the server from known vulnerabilities.

Our review of DTMB's Configuration Management Database (CMDB) noted that 11 (41%) of the 27 UNIX operating system versions were unsupported. These unsupported versions were operational on approximately 30 (3%) of the State's 950 UNIX servers, some of which contained applications considered critical to State government operations and life threatening to citizens if unavailable. On average, operating system versions were unsupported for 7.2 years, with 5 versions being unsupported for over 10 years. The following chart depicts the number of years each operating system version has been operational in the State's server environment since it became unsupported:



* See glossary at end of report for definition.

Because these operating systems were unsupported and not using current versions, DTMB's automated tool for detecting vulnerabilities could not be installed on these servers.

DTMB informed us that the use of unsupported operating system versions occurred because the State's executive branch departments maintain legacy applications in the consolidated hosting center until the application can be architected and refreshed. DTMB has an architectural roadmap that does identify supported operating system versions. DTMB also informed us that it is implementing a new IT infrastructure, the Next Generation Digital Infrastructure* (NGDI), which will define the acceptable UNIX operating systems and require those State executive branch departments transitioning to NGDI to use these operating systems.

RECOMMENDATION

We recommend that DTMB establish a strategy to ensure that only supported UNIX operating system versions are installed on servers containing the State's applications.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will establish a strategy to ensure that only supported UNIX operating system versions are installed on servers containing the State's applications. DTMB will utilize the Enterprise Architecture Roadmap to identify authorized and supported operating systems. Owners of any unauthorized and unsupported operating systems will be issued a "Notice of Non-Compliance," which will be reported for further resolution. DTMB will ensure that new operating system installations comply with the Enterprise Architecture Roadmap. In addition, DTMB is implementing NGDI, which will define acceptable UNIX operating systems and require State executive branch departments transitioning to the NGDI to use these operating systems.

* See glossary at end of report for definition.

FINDING #3

Improved patch management controls would help protect State applications from known vulnerabilities and ensure data integrity.

DTMB did not apply operating system patches in a timely manner according to its policy. UNIX servers had not been updated with the latest patches to protect operating systems from known security and system vulnerabilities and ensure data integrity.

DTMB Technical Standard 1345.00.50 requires that quarterly updates be performed to enhance server security and safeguard data against attack or intrusion.

Our review of patch management controls over the State's approximately 950 UNIX servers disclosed:

- a. For 53 (90%) of 59 judgmentally selected servers, DTMB did not install patches in a timely manner. As a result, the servers were not fully protected from known security exploits, leaving them vulnerable to attacks.
- b. Patch management maintenance windows were not specifically defined between DTMB and State executive branch departments in 559 (58%) of the servers identified in the CMDB. Without specifically defined maintenance windows, server administrators cannot effectively prioritize and apply patches in a timely manner.

DTMB informed us that it relies on a manual process to apply patches and that the maintenance windows allocated to it by State executive branch departments are infrequent and insufficient to apply patches. Also, DTMB informed us that it is implementing an automated process for applying patches, but manual intervention is continuously required to ensure that the automated process is working effectively. In addition, DTMB informed us that NGDI will define standard maintenance windows for all servers and require executive branch departments transitioning to NGDI to allow patching to occur during these windows.

RECOMMENDATIONS

We recommend that DTMB apply operating system patches in a timely manner according to its policy.

We also recommend that DTMB consider fully designing and implementing an automated patch management control process and define patch maintenance windows with State executive branch departments.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendations and will use an automated patch management control process and tools to patch servers, at a minimum quarterly, and run reports to identify any deficient patches. In addition, DTMB will establish and implement a memorandum of understanding (MOU), with

all executive branch agencies, to define mutually agreed upon patch management maintenance windows. Lastly, DTMB will enforce DTMB procedure 1345.00.50.08 on Server Patch Management, to ensure servers are patched timely, with any exceptions receiving a "Notice of Non-Compliance," which will be reported for further resolution.

FINDING #4

Improvements needed to UNIX operating system access controls.

DTMB did not establish and implement effective access controls over the State's UNIX operating systems to help prevent or detect inappropriate access to data.

DTMB Administrative Guide policy 1335, Information Technology Access Control, requires the establishment of a process to control and document the assignment of access rights based on current job responsibilities and to allow access to be managed, controlled, and periodically reviewed to ensure that access is based on the principle of least privilege*. To safeguard access authentication, the policy also requires that passwords be regularly changed.

Our review of access controls on 63 judgmentally selected UNIX servers disclosed:

- a. An ineffective process for granting access to UNIX servers:
 - (1) The DTMB-3543, UNIX/LINUX user ID request form, authorizes and grants access to UNIX servers. However, use of this form was not required in a formal DTMB procedure. For 53 (84%) of the 63 servers, this form was not completed for at least 1 and up to 4 users on a single server.
 - (2) User access was not based on the principle of least privilege. For 11 (17%) of the 63 servers, we identified at least 1 and up to 3 users with inappropriate access. For 42 (67%) of the 63 servers, we were unable to determine the appropriateness of user access for at least 1 and up to 4 users on a single server because of the lack of user ID request forms.
- b. An ineffective process for granting users elevated rights to UNIX servers:
 - (1) DTMB had not developed a standardized form for authorizing elevated rights and, because of limited search functionality, DTMB could not produce a record of its authorization for at least 1 and up to 24 users with elevated rights on 36 (57%) of the 63 servers.
 - (2) Elevated user rights were not based on the principle of least privilege. We determined that, for 17 (27%) of the 63 servers, at least 1 and up to 2 users on a single server were inappropriately granted elevated rights. On 36 (57%) of the 63 servers, we were

* See glossary at end of report for definition.

unable to determine the appropriateness of elevated rights granted to at least 1 and up to 24 users on a single server because of the lack of approval documentation. These elevated rights allow the users to obtain complete control of the operating system.

- c. The lack of an effective periodic access review to ensure the appropriateness of user access.

DTMB informed us that each UNIX administrator reviews a list of user accounts and users granted elevated rights weekly for the servers he or she is responsible for managing. However, DTMB did not follow up with management to determine if access rights remained appropriate. Also, DTMB did not have a process in place in the UNIX server environment to identify when an individual ends employment with the State. Without effective periodic access review, DTMB cannot efficiently ensure that user access rights are based on the principle of least privilege.

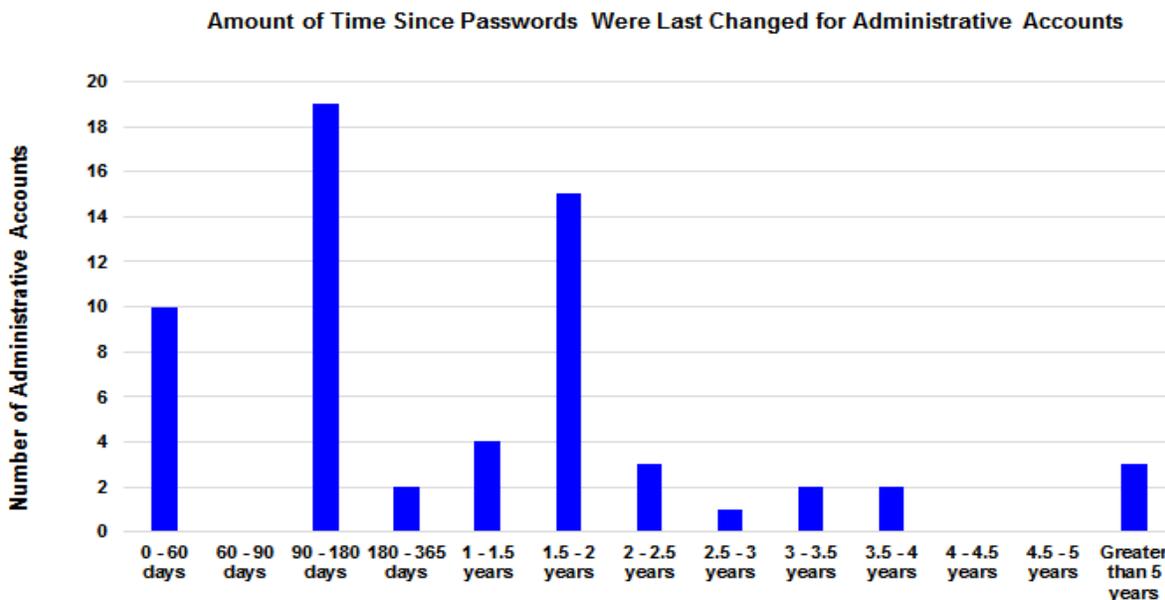
- d. Ineffectively implemented password controls on the UNIX servers:

- (1) Passwords were not changed in a timely manner. DTMB Technical Standard 1335.00.03 requires that passwords have a 90-day maximum life. Also, DTMB's baseline configuration* for 2 of the 5 UNIX operating system versions reviewed requires that passwords have a 60-day or 63-day maximum life, respectively. Our review disclosed:

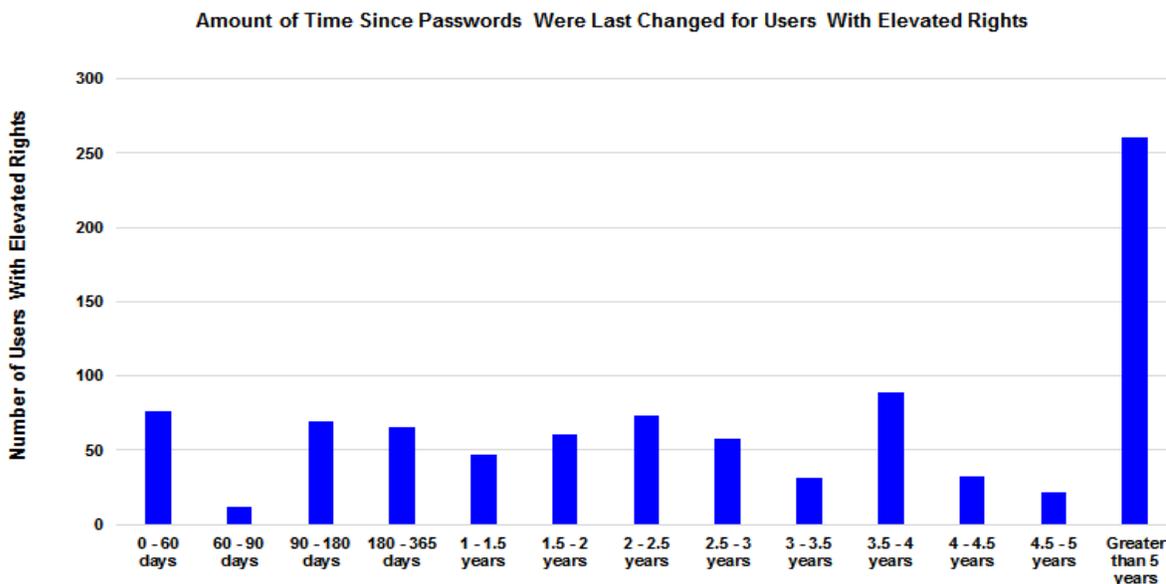
- (a) The password for the administrative account had not been changed in a timely manner for 51 (84%) of the 61 servers. Also, the password change requirement for the administrative account on one server had been manually adjusted to bypass the password change control. The following chart depicts the amount of time since the password for the administrative account had been changed, with the greatest

* See glossary at end of report for definition.

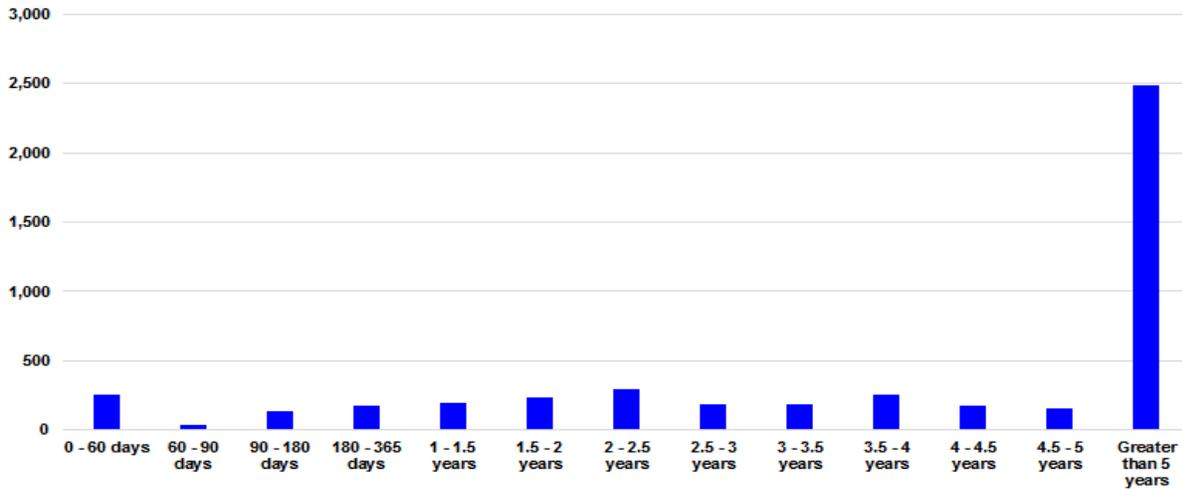
lapse in password change for an administrative account being approximately 9 years:



(b) Active users did not change their passwords in a timely manner on 63 (100%) of the 63 servers. The following charts depict the amount of time since users with elevated rights had changed their passwords, with the greatest lapse in password change for a user with elevated rights being approximately 11 years, and the amount of time since all accounts had their passwords changed:



Amount of Time Since Passwords Were Last Changed for All Accounts



- (2) DTMB did not timely change the passwords for the two databases* containing the administrative passwords.
- (3) On 4 (6%) of the 63 servers, DTMB did not enforce the creation of passwords for at least 1 and up to 2 users on a single server. Without a password, these user accounts may be accessed without any authentication control.

The conditions noted in this finding occurred because DTMB did not effectively follow its policies related to access controls.

RECOMMENDATION

We recommend that DTMB establish and implement effective access controls over the State's UNIX operating systems.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and has updated its elevated user rights procedure to more effectively control access to the UNIX operating systems. In addition, DTMB is in the process of implementing an elevated rights and directory services software tool; updating associated access procedures; and developing new reports and monitoring processes to further strengthen UNIX operating system access controls and ensure compliance with DTMB policy.

* See glossary at end of report for definition.

ESTABLISHING EFFECTIVE GOVERNANCE STRUCTURE

BACKGROUND

The DTMB Technical Services Division includes UNIX server teams that manage the State's UNIX servers. The server teams are made up of server administrators who are responsible for managing the operating system of their assigned servers. Also, DTMB created the Cloud Automation and Audit Compliance teams to provide oversight and support for UNIX security.

AUDIT OBJECTIVE

To assess the effectiveness of DTMB's efforts to establish an effective governance structure over the State's UNIX server environment.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DTMB established and implemented some policies, standards, and procedures related to security of the UNIX server environment.
- DTMB has taken the initial steps to implement automated security tools in its UNIX server environment.
- DTMB contracted with a third party to perform an enterprise risk assessment of the State's IT environment.
- One material condition (Finding #5) related to detection and remediation of security vulnerabilities.
- Two reportable conditions (Findings #6 and #7) related to segregation of duties* and inventory management.

* See glossary at end of report for definition.

FINDING #5

Enhancements to procedures for detecting and remediating security vulnerabilities are necessary.

DTMB did not fully establish and implement effective procedures to detect and remediate security vulnerabilities to ensure that the State's UNIX servers cannot be exploited to gain elevated privileges.

COBIT recommends that policies and procedures define baseline configurations, internal control*, security, and confidentiality. To direct the State toward maintaining the highest possible level of server security, DTMB established Technical Standard 1340.00.03. This standard identifies configuration hardening* and vulnerability scanning as two key components of IT resource management. It further requires that scanning be performed monthly and all moderate to severe security vulnerabilities detected be remediated.

Our review of DTMB's process to detect and remediate UNIX server vulnerabilities disclosed:

- a. Vulnerability scans, using the State's current vulnerability management tool, did not detect whether critical configuration settings, identified by DTMB and industry best practices, were implemented.

Examples of security vulnerabilities not detected by the scanning of servers include password configurations, log-in configurations, file permissions, and user account configuration management*.

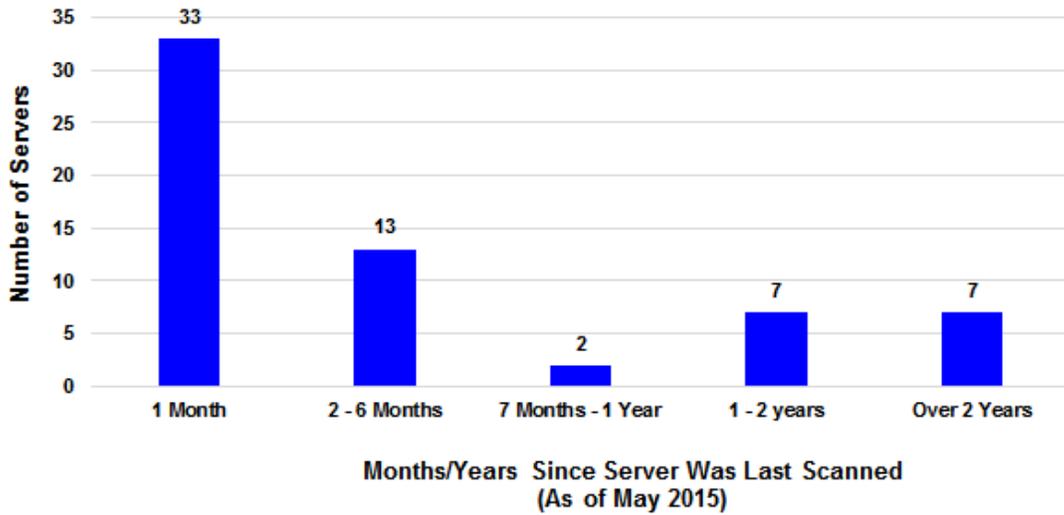
- b. Vulnerability scans were not performed monthly on all UNIX servers. Therefore, DTMB did not remediate vulnerabilities in a timely manner.

As of May 2015, 29 (47%) of the 62 servers in operation had not been scanned in over a month.

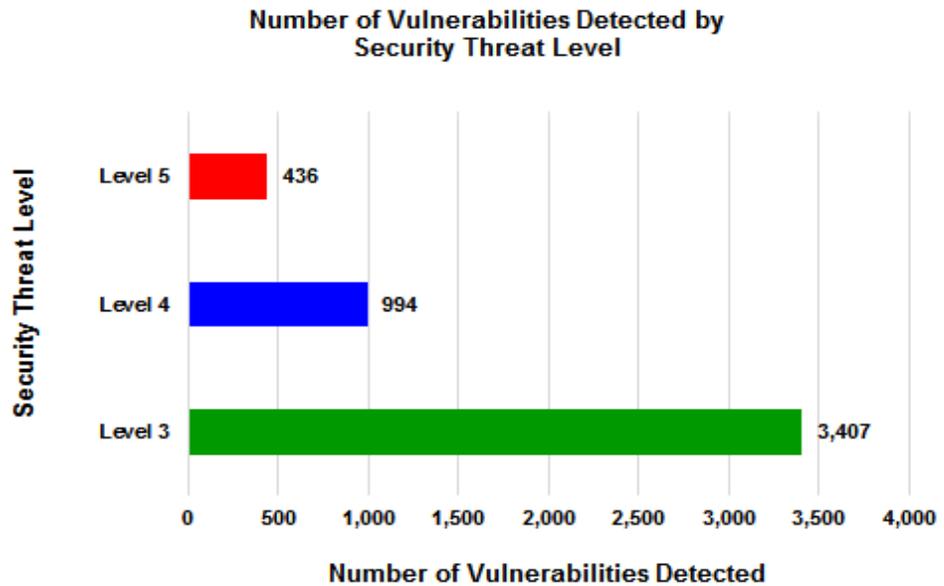
We judgmentally selected 63 UNIX servers, of which 62 servers were in operation for over a month as of May 2015, and noted that 29 (47%) of the 62 servers had not been scanned in over one month. The following

* See glossary at end of report for definition.

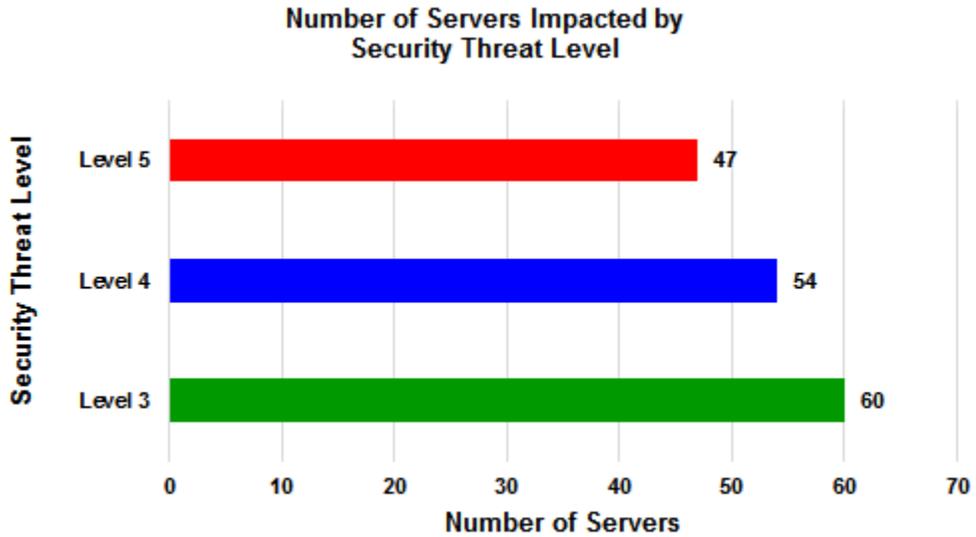
chart identifies the number of months or years since each of the 62 servers were last scanned:



In addition, we requested DTMB to provide us the vulnerability scans for all 63 servers between July 6, 2015 and August 13, 2015. These scans identify security threats* in 5 levels with 5 being the highest level of risk and 1 being the lowest. The following charts summarize the number of vulnerabilities detected and number of servers impacted for threat levels 3 through 5:



* See glossary at end of report for definition.



The following chart summarizes the average number of vulnerabilities detected per server and identifies the highest number of vulnerabilities detected in that security threat level on a single server.

| Security Threat Level | Average Number of Vulnerabilities Detected Per Server | Highest Number of Vulnerabilities Detected on a Single Server |
|-----------------------|---|---|
| Level 3 - Level 5 | 77 | 420 |
| Level 5 | 7 | 34 |
| Level 4 | 16 | 87 |
| Level 3 | 54 | 310 |

DTMB informed us that not all threats detected in the vulnerability scans are within the DTMB Technical Services Division's control and may require the assistance of other areas within DTMB, such as the Agency Services Division or the Telecommunications Division, to remediate the vulnerabilities. DTMB also informed us that it is developing a process to assign responsibilities for remediation of threats detected in the vulnerability scans.

- c. Security baseline configurations were not fully established by DTMB.

Baselines define the recommended configuration settings that will reduce security risks to an acceptable level. We noted:

- (1) DTMB did not adopt a UNIX security configuration checklist. NIST special publication 800-70 revision 2 states that organizations should use security configuration checklists to reduce the number of vulnerabilities that attackers can attempt to exploit and lessen the impact of successful attacks. NIST also identifies a repository that contains industry best practice security configuration checklists, such as those released by the Center for Internet Security* (CIS) or the Defense Information Systems Agency (DISA). DTMB had adopted guidance published by NIST but had not adopted security checklists into its standard procedures.
- (2) Hardening procedures, designed to ensure that appropriate server security is in place before a server is deployed in the production environment, were not established for two UNIX versions. Also, three procedures did not meet industry best practice recommendations for certain configuration settings.

Server automation tool used for detecting and remediating security vulnerabilities was not installed on all UNIX servers.

- d. The server automation tool purchased by DTMB to help detect operating system vulnerabilities was not installed on all servers.

DTMB entered into purchase orders for approximately \$2.9 million between October 2013 and August 2015 on software licensing, maintenance, training, and support for a server automation tool for detecting and remediating security vulnerabilities on servers. We noted that 4 (6%) of the 63 judgmentally selected servers did not have the server automation tool installed. DTMB also informed us that, as of May 2015, it had not installed the server automation tool on an additional 132 servers.

DTMB informed us that it is in the process of selecting a baseline configuration and utilizing its automated tool to scan UNIX servers against the baseline. Also, DTMB informed us that all servers which transition to NGDI will receive scans on a regular basis.

RECOMMENDATIONS

We recommend that DTMB fully establish and implement effective procedures to detect and remediate security vulnerabilities on UNIX servers.

* See glossary at end of report for definition.

We also recommend that DTMB fully develop and implement a process for assigning roles and responsibilities for the remediation of threats detected by monthly vulnerability scans.

**AGENCY
PRELIMINARY
RESPONSE**

DTMB provided us with the following response:

DTMB agrees with the recommendations and has purchased the necessary automation tools and initiated a project to install the tools on all UNIX servers. The new tools will automate the detection and remediation of security vulnerabilities. DTMB is developing a process to assign responsibilities, between Technical Services, Agency Services, and Network and Telecommunications Division, for the remediation of threats detected in vulnerability scans. In addition, DTMB will utilize existing server management standards, new vulnerability scan procedures, new monitoring processes, and new operational compliance reports to enhance the detection and remediation of security vulnerabilities. All procedures will be reviewed at least annually to meet industry best practices.

FINDING #6

Segregation of duties could help ensure that critical operating system controls cannot be bypassed.

DTMB did not fully establish a segregation of duties over the administration of UNIX servers. The DTMB Agency Services Division had too much control over key processes, which increased the risk that controls designed to secure the State's information systems could be circumvented.

COBIT states that segregation of duties should be established to ensure that individuals in critical positions cannot bypass controls. It would also help ensure the oversight and secure configuration of UNIX servers.

DTMB assigned the responsibility for UNIX server administration to the Technical Services Division and assigned the responsibility for application and database administration and development to the Agency Services Division.

Our review of UNIX server administration disclosed:

- a. The DTMB Agency Services Division contracted with a third party vendor for the server administration function of a system. While the vendor is organizationally located within the Technical Services Division, the vendor reports to and is managed by the Agency Services Division. The Agency Services Division's management of this vendor is a conflict of interest between application and operating system administration because it creates an increased risk that critical operating system controls could be bypassed (see observation* related to vendor administration of UNIX servers).
- b. Employees within the DTMB Agency Services Division acted as server administrators for two UNIX servers. DTMB should transfer server administration functions to the Technical Services Division to ensure adequate oversight. We reported this lack of segregation of duties in our performance audit of Statewide UNIX Security in 2010. At that time, DTMB informed us that it would pursue transitioning servers to the Technical Services Division's control.

These weaknesses occurred because of the Technical Services Division not enforcing its responsibility for administration of these servers.

RECOMMENDATION

We recommend that DTMB fully establish a segregation of duties over the administration of UNIX servers.

* See glossary at end of report for definition.

**AGENCY
PRELIMINARY
RESPONSE**

DTMB provided us with the following response:

DTMB agrees with the recommendation and will fully establish segregation of duties over the administration of UNIX servers.

FINDING #7

Inventory management improvements are needed to ensure that critical decisions can be made in a timely manner for the State's information systems.

DTMB did not maintain an accurate record of UNIX server information to help ensure server security and availability of information for critical business decisions. This information includes whether the server supports a critical application for the State of Michigan, the level of security applicable to the server, and what security guidelines are applicable to the specific UNIX version.

DTMB established the CMDB as the official inventory of server information. DTMB Technical Standard 1345.00.50 states that all server hardware and software used for the purpose of State business will be fully documented in the CMDB. Also, COBIT states that an inventory should be established and maintained to ensure that owners are able to make business decisions.

Our review of selected information in the CMDB as of June 2015 disclosed:

a. Incomplete information in the CMDB.

The CMDB did not always identify which systems resided on each server, the security zone the server resides in, the UNIX version, and other information needed to maintain the servers.

b. Inaccurate information in the CMDB.

We judgmentally selected 43 servers and noted that the CMDB contained inaccurate operating system version information for 17 (40%) of the 43 servers. Also, we noted 1 instance in which a server was identified as operational but was no longer in use. In addition, we noted differences among operating system, operating system family, and the operating system used for billing purposes for a server.

To improve the completeness and accuracy of its inventory, DTMB entered into purchase orders for approximately \$986,000 on an automated inventory management tool. This tool has been installed on the majority of the State's servers and is in the process of being fully implemented. We noted that this tool reported select information more accurately than the server information contained in the CMDB.

DTMB informed us that incomplete and inaccurate information in the CMDB is the result of a manual process not being followed properly or not being followed at all when changes are made to the server.

RECOMMENDATIONS

We recommend that DTMB maintain an accurate record of UNIX server information.

We also recommend that DTMB develop a process to fully utilize an automated tool to help manage its UNIX server inventory.

**AGENCY
PRELIMINARY
RESPONSE**

DTMB provided us with the following response:

DTMB agrees with the recommendations and has procured an automated inventory management tool which is in the process of being fully implemented. The automated inventory management tool will automatically confirm and update the State's information systems inventory data in the CMDB.

OBSERVATION #1

Transferring server administration function from the third party vendor to DTMB could result in cost savings.

DTMB contracted with a third party vendor in 2009 for administration of certain UNIX servers at an annual cost of approximately \$264,000. The contract required that the vendor transfer server administration knowledge to the State so that the State could support and maintain the servers on an ongoing basis. In 2014, DTMB exercised its option to renew the contract for an additional year.

Despite the DTMB Technical Services Division having 16 classified employees capable of performing server administration functions on all UNIX operating system versions, as of August 2015, server administration was still performed by the vendor. Transferring server administration from the third party vendor to State employees could result in cost savings.

AGENCY DESCRIPTION

DTMB maintains and operates 27 variations of UNIX operating systems on approximately 950 UNIX servers. Systems and data critical for the operation and oversight of State government reside on these servers including systems for:

- Processing services and payments to citizens in need.
- Tracking and managing road and bridge construction projects and payments.
- Maintaining prisoner, parolee, and probation information.
- Processing the State employee payroll.

UNIX servers also provide a variety of enterprisewide 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.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records related to the State's UNIX operating system controls. 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.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered the period October 1, 2012 through August 31, 2015.

METHODOLOGY

We conducted a preliminary survey of DTMB's governance structure and controls over UNIX operating systems to formulate a basis for defining our audit objectives and scope. During our preliminary survey, we:

- Conducted interviews to obtain an understanding of DTMB's operations, activities, and internal control.
- Obtained an understanding of DTMB's policies, standards, and procedures related to UNIX servers.
- Analyzed UNIX server inventory information and automated reports.
- Reviewed a draft of a contractor-prepared enterprise risk assessment.

OBJECTIVE #1

To assess the effectiveness of DTMB's efforts to implement security and access controls over the State's UNIX servers.

To accomplish our first objective, we:

- Interviewed DTMB UNIX server team managers to obtain an understanding of security and access controls implemented for UNIX operating systems.
- Judgmentally selected 63 UNIX servers critical to State government operations and tested the appropriateness of access controls.

* See glossary at end of report for definition.

- Compared server configurations with DTMB policies and industry best practices for 59 of the 63 servers.
- Analyzed DTMB's server inventory to identify unsupported versions of UNIX operating systems.
- Analyzed and tested DTMB's patch management process for 59 of the 63 servers.

OBJECTIVE #2

To assess the effectiveness of DTMB's efforts to establish an effective governance structure over the State's UNIX server environment.

To accomplish our second objective, we:

- Interviewed DTMB management to obtain an understanding of DTMB's governance structure over the State's UNIX server environment.
- Obtained and reviewed DTMB vulnerability scans for the 63 selected UNIX servers to assess DTMB's processes for monitoring UNIX servers and remediating security vulnerabilities.
- Tested DTMB's policies, standards, and procedures against industry best practices.
- Reviewed and assessed the accuracy and completeness of UNIX server information in the CMDB, which is an inventory of the State's automated systems.

CONCLUSIONS

We base our conclusions on our audit efforts and the resulting material conditions and reportable conditions.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve State government operations. Consequently, we prepare our performance audit reports on an exception basis.

AGENCY RESPONSES

Our audit report contains 7 findings and 10 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all 10 recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion at the end of 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 an audited agency to develop a plan to comply with the 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.

**PRIOR AUDIT
FOLLOW-UP**

We released our prior performance audit of Statewide UNIX Security, Department of Technology, Management, and Budget (084-0563-09), in April 2010. We rewrote all 5 prior audit recommendations for inclusion in Findings #1, #4, #6, and #7 of this audit report.

GLOSSARY OF ABBREVIATIONS AND TERMS

| | |
|---|---|
| access controls | Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts. |
| availability | Timely and reliable access to data and information systems. |
| baseline configuration | A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. |
| Center for Internet Security (CIS) | 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. |
| CMDB | Configuration Management Database. |
| confidentiality | Protection of data from unauthorized disclosure. |
| configuration | The way a system is set up. Configuration can refer to either hardware or software or the combination of both. |
| configuration management | The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system. |
| 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. |
| database | A collection of information that is organized so that it can be easily accessed, managed, and updated. |
| DTMB | Department of Technology, Management, and Budget. |
| effectiveness | Success in achieving mission and goals. |

| | |
|---|--|
| hardening | Configuring an operating system and applications to reduce security weaknesses. |
| information technology (IT) | Anything related to computing technology, such as networking, hardware, software, the Internet, or the people who work with these technologies. |
| integrity | Accuracy, completeness, and timeliness of data in an information system. |
| internal control | The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of assets against unauthorized acquisition, use, or disposition. |
| material condition | A matter that, in the auditor's judgment, is more severe than a reportable condition and 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. |
| Next Generation Digital Infrastructure (NGDI) | The State's private cloud-based infrastructure that is composed of computer, storage, network, and data protection platforms. |
| observation | A commentary that highlights certain details or events that may be of interest to users of the report. An observation differs from an audit finding in that it may not include the attributes (condition, effect, criteria, cause, and recommendation) that are presented in an audit finding. |
| 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. |
| patch | An update to an operating system, applications, or other software issued specifically to correct particular problems with the software. |

| | |
|------------------------------|---|
| 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. |
| principle of least privilege | The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes. |
| 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 to have occurred. |
| security | Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity. |
| segregation of duties | Segregation of the management or execution of certain duties or areas of responsibility to prevent or 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. |

