STATE OF MICHIGAN
DEPARTMENT OF COMMUNITY HEALTH

RICK SNYDER
GOVERNOR

JAMES K. HAVEMAN
DIRECTOR

September 20, 2012

Mr. Doug Ringler
Office of Internal Audit Services
Office of the State Budget
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, Michigan 48913

Dear Mr. Ringler:

In accordance with the State of Michigan, Financial Management Guide, Part VII, attached are the final summary table identifying our responses and corrective action plans to address recommendations contained within the Office of the Auditor General's Performance Audit of the Michigan Women, Infants, and Children Information System (MI-WIC).

Questions regarding the summary table or corrective action plans should be directed to me at (517) 373-1508 or Myersp3@michigan.gov.

Sincerely,

Signature Redacted

Pam Myers, Director
DCH Office of Audit

Enclosure

Cc: Office of the Auditor General   House Appropriations Committee
        House Fiscal Agency   House Standing Committee
        Senate Fiscal Agency   Senate Appropriations Committee
        Executive Office   Senate Standing Committee
        DCH, James K. Haveman   DCH, Nick Lyon
        DCH, Timothy Becker   DCH, Stan Bien
        DCH, Karla Garcia

PERFORMANCE AUDIT OF THE
MICHIGAN WOMEN, INFANTS, AND CHILDREN
INFORMATION SYSTEM (MI-WIC)

DEPARTMENT OF COMMUNITY HEALTH AND

DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

JANUARY 2012

AUDIT RESPONSE

Approved: _____

Tim Becker, Senior Deputy Director
Department of Community Health, Operations Administration

Date: _07/31/2012_

AUDIT REPORT SUMMARY

DEPARTMENT: Community Health

AUDIT PERIOD: October 1, 2009 – September 30, 2011

REPORT DATED: January 18, 2012

DISPOSITION OF AUDIT RECOMMENDATIONS

	CITATIONS COMPLIED WITH	CITATIONS TO BE COMPLIED WITH	CITATIONS DCH DID NOT AGREE WITH
Recommendation #1: OAG recommended that DCH, in conjunction with DTMB, effectively monitor the third party vendor's security configuration of the MI-WIC database.	X		
Recommendation #2: OAG recommended that DTMB, in conjunction with DCH, fully establish security controls over the MI-WIC database.	X	2.c.	
Recommendation #3: OAG recommended that DTMB fully establish effective security and access controls over the MI-WIC operating system.	3.b., 3.d.	X	
Recommendation #4: OAG recommended that DCH document authorization for user access to MI-WIC for selected high-risk State level MI-WIC users.	X		

Recommendation 1:   Database Security Management

OAG recommended that DCH, in conjunction with DTMB, effectively monitor the third party vendor's security configuration of the MI-WIC database.

Response:

DTMB and DCH have worked to effectively monitor the security configurations of the MI-WIC database.   DTMB and DCH have evaluated the MI-WIC database software installation, configuration and patching levels and recommended the appropriate remediation actions. As a result, DTMB in conjunction with DCH WIC has worked with the vendor (3SSW), to install the most current approved Oracle Security Patches, which the vendor completed in May 2012. The vendor has also upgraded the MI-WIC Oracle software from 10G to 11G in the staging environment in May 2012. Production and disaster recovery environment upgrades are ongoing and will be completed in August 2012. Lastly, DTMB, in conjunction with DCH WIC, implemented a policy of applying Oracle patches in accordance with DTMB's quarterly installation schedule.

Recommendation 2:   Database Security and Access Controls

OAG recommended that DTMB, in conjunction with DCH, fully establish security controls over the MI-WIC database.

Response:

DTMB and DCH have worked to fully establish security controls over the MI-WIC database.

With regard to part a., DTMB provided DCH WIC with a SOM policy regarding database access in May 2012. DCH WIC has implemented the processes for granting, maintaining, and monitoring database user accounts and roles as stated in part b. of this response.

With regard to part b., DCH WIC developed/implemented database security processes and forms, including approval, maintaining, and monitoring procedures. As of April 2012, all database user access and role membership forms have been reviewed and granted approval by DCH WIC.   MI-WIC database access process is managed by the DCH WIC System Administrator.

With regard to part c., DTMB will provide the approved standard for configuration parameters and the process for reviewing profile and database configuration settings to DCH WIC by August 15, 2012. DTMB, in conjunction with DCH will work with the vendor to modify database configuration settings accordingly in MI-WIC staging, production and DR database environments by August 31, 2012.

With regard to part d., DCH WIC has completed the review of database account access and database roles and granted approval to appropriate users in April 2012. DCH WIC has reviewed

and approved a Database Access Form and the vendor only provides access to the MI-WIC staging, production, and DR database environments as approved for specific user role. DTMB will provide network connection if needed based on DCH approval.

With regard to part e., DTMB and DCH evaluated the feasibility of Oracle database encryption in July 2012. DCH has purchased the necessary encryption software; however, other DCH program data is at a higher risk for disclosure. Those programs will take precedence over MIWIC data. DCH in conjunction with DTMB may at a later date determine that encryption of the MIWIC data is necessary.

With regard to part f., DCH has approved the change in configuration settings for the Oracle audit trail for monitoring individual database user accounts and user activity. In April 2012, the vendor implemented the maintenance of audit logs in the database and creates quarterly reports. The DCH WIC System Administrator has begun using the audit log report to monitor database activity quarterly as of May 2012.

Recommendation 3:   Operating System Security and Access Controls

OAG recommended that DTMB fully establish effective security and access controls over the MI-WIC operating system.

Response:

DTMB is working to fully establish effective security and access controls over the MI-WIC database operating systems and will provide timely progress reports to DCH WIC on the action items noted below.

With regard to part a., DTMB has a project in progress to use the Center for Internet Security Configuration Assessment Tool (CIS-CAT) for proactive system auditing. The CIS-CAT tool will help DTMB to monitor file permissions and other system settings and the tool will be fully implemented by December 2012. In addition, DTMB has restricted the default UMASK upon testing the changes in the development environment as of May 2012.

With regard to part b., DTMB has properly restricted the root account from logging in remotely as of November 2011.

With regard to part c., DTMB has started a Lightweight Directory Access Protocol (LDAP) project to centralize account controls and will further restrict password controls during the LDAP conversion. The estimated time of implementation is December 2012.

With regard to part d., DTMB now has standard build documentation and needs to expand the document to include cluster services. Applications needing disabled services to run must submit a DIT-400 (exception form) which will be reviewed by the Technical Review Board (TRB) or

Enterprise Technical Review Board (ETRB). In addition, DTMB uses the Volume Manager Service for cluster services and Network File Systems (NFS). DTMB has all necessary documentation regarding enabled services and exception justification as of January 2012.

With regard to part e., SSH settings have been corrected and are now implemented in our standard build. Systems built prior to the development of the SSH settings standard build process are in the process of being corrected. The estimated time of implementation is December 2012.

With regard to part f., DTMB has begun a Lightweight Directory Access Protocol (LDAP) project to centralize account controls with an estimated time of implementation of December 2012. Other controls implemented include the utilization of the DIT-161 form, filled out by the manager and submitted by an Authorized Requester, for user additions, deletions, or modifications. DTMB also has as a Separation of Duties Standard as a work in progress. Database Administrator's (DBA) are required to request elevated rights with a reason via a Remedy ticket. In addition, DBA's are only allowed root access during the build process and temporarily during application updates/upgrades. Lastly, as of December 31, 2011, DTMB has implemented a Central Monitoring process that monitors users' with access to privileged accounts.

Recommendation 4:   Application Access Controls

OAG recommended that DCH document authorization for user access to MI-WIC for selected high-risk State level MI-WIC users.

Response:

DCH WIC has established and documented the authorization process for access control for the MI-WIC application for all system users. The system solution for this process was implemented in the MI-WIC release 5.1 which was successfully implemented in the production environment as of April 2012. The system solution will allow State staffs to more effectively monitor user authorization and user access to MI-WIC. The process to implement authorization of user access has been documented for all application users as of April 2012.