STATE OF MICHIGAN

RICK SNYDER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

DAVID B.BEHEN
DIRECTOR

July 24, 2017

RECEIVED

JUL 28 2017

AUDITOR GENERAL

Rick Lowe, Director
Office of Internal Audit Services
State Budget Office
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, Michigan 48913

Dear Mr. Lowe:

In accordance with the State of Michigan, Financial Management Guide, Part VII, attached is a summary table identifying our responses and corrective action plans to address recommendations contained within the Office of the Auditor General's audit report of the Department of Technology, Management and Budget, Disaster Recovery and Business Continuity of IT Systems.

Questions regarding the summary table or corrective action plans should be directed to me.

Sincerely,

Signature Redacted

Michael Gilliland, Director
DTMB Financial Services

c: Representative Laura Cox, Chair, House Appropriations
Senator Dave Hildenbrand, Chair, Senate Appropriations
Melissa Schuiling, Office of the Auditor General
Dick Posthumus, Executive Office
Darin Ackerman, Executive Office
House Fiscal Agency
Senate Fiscal Agency
Brom Stibitz, DTMB
Rodney Davenport, DTMB
John Juarez, DTMB
Kerri DeBano, DTMB
Phillip Jeffery, DTMB
David Bates, DTMB
Caleb Buhs, DTMB
Mike Williams, SBO

Disaster Recovery and Business Continuity of IT Systems
Agency responses and corrective action plans

Summary of Agency Responses to Recommendations

1. Audit recommendations DTMB fully complied with: Findings 2, 3, 4, 5, 7, and 8
2. Audit recommendations DTMB agrees with and will comply: Findings 1 and 6
3. Audit recommendations DTMB disagrees with: None

Agency Responses to Recommendations

Finding #1: More complete IT disaster planning needed:
DTMB agrees with the recommendation and plans to restore all critical infrastructure services and enterprise systems necessary to restore the other Red Card systems in the event of a Statewide IT disaster. BCPs and DRPs for all critical infrastructure systems and enterprise systems will be completed and maintained. Plans for all critical systems currently on the Red Card have been developed and are in LDRPS. DTMB has developed a business impact analysis (BIA) to help with prioritizing systems (.e.g. Active Directory, LDRPS, etc.) by assigning a score based on business owner responses to a questionnaire. In addition, DTMB has developed a tiering methodology to address restoration priority, recovery time objectives, and recovery point objectives. DTMB has identified a solution for ensuring all plans are completed and stored in LDRPS. DTMB's Network and Telecommunications division is developing a recovery plan for the network and intranet to be stored in LDRPs. DTMB's migration from LDRPS to a new a state-hosted system is moving forward with a project completion date for May 2018. In addition, more comprehensive test plans from an enterprise view will be developed and tests will be scheduled on a regular basis. DTMB will comply with the recommendation by September 1, 2017.

Finding #2: Completeness and accuracy of the Red Card should be improved.
DTMB agrees with and has complied with the recommendation. DTMB will continue to work with State agencies to ensure the completeness and accuracy of the Red Card by determining the most critical systems and services for their inclusion on the Red Card. DTMB is working with State agencies to identify, validate, and approve the State's listing of critical systems and services, through the completion of a business impact analysis (BIA), for their inclusion on the Red Card. Inclusion on the Red Card is now required for Tier 1 and 2 systems and services. DTMB requires that all agency partnership agreements identify an agency's critical applications; and requires State agency management approval when systems are added to, removed from or reclassified on the Red Card. In addition, DTMB will continue to assist State agencies in understanding the

importance of complete BCPs and DRPs through BCP/DR 101 training. DTMB held two separate BCP/DR 101 sessions in late 2016 and additional sessions are planned for the fall 2017.

Finding #3: Better coordination of plan preparation needed.
DTMB agrees with and has complied with the recommendation. In 2016, DTMB began a department-wide initiative to address existing internal control weaknesses in the State's information technology operations, referred to as the Material Internal Control Weaknesses Remediation and Accountability Program (MICWRAP). As part of this initiative, DTMB has now completed 100% of the department's DRPs for 34 Red Card applications. Also from this effort, DRPs for 100% of other agencies' Red Card applications have been completed. DTMB will continue to assist state agencies in completing a business impact analysis to identify their critical, non-red card, applications and coordinate the preparation of remaining DRPs and BCPs. DTMB will also assist State agencies in understanding the importance of complete BCPs and DRPs through the BCP/DRP 101 training. In May 2017, DTMB established and filled the "Statewide Business Continuity Coordinator" position to coordinate the preparation of BCPs with State agencies and DTMB Agency Services. In addition, DTMB will ensure there is adequate staffing available in the event of an emergency.

Finding #4: DRPs and BCPs should be reviewed for completeness.
DTMB agrees with and has complied with the recommendation. As part of the MICWRAP initiative, the department has developed and completed a "content and validity" review of all DR and BC plans. The review helped to ensure DR and BC plans contain the necessary elements for effective disaster recovery. DTMB has reviewed all hosting center BCPs and all critical elements have been included. In addition, DTMB has revised DRP and BCP training to help ensure all of the necessary elements are documented and contained in the DRP and BCPs. DTMB has also created a training schedule for providing the BCP/DR 101 training to State agencies. DTMB held two separate BCP/DR 101 sessions in late 2016 and additional sessions are planned for the fall 2017.

Finding #5: More DR servers needed.
DTMB agrees with and has complied with the recommendation. DTMB will continue to work with State agencies to ensure that DR servers are in place for all Red Card systems. DTMB has now completed 100% of the department's DRPs for 34 Red Card applications. Also from this effort, DRPs for 100% of other agencies' Red Card applications have been completed. DTMB will continue to assist State agencies in completing a business impact analysis (BIA) to identify their critical systems; coordinate the preparation of DRPs and BCPs; and

communicate the importance of funding DR servers. DTMB, working with State agencies, uses information from the BIA to determine the system's level of criticality, based on the BIA tier scores, which turn is used to determine the required level of support, including the level of redundant hardware required. . Inclusion on the Red Card is now required for Tier 1 and 2 systems and services. A "notification of non-compliance", per Standard 1345.00.14, is now issued to a critical system that is identified as needing to be on the state's Red Card, but not having the required disaster recovery elements.

Finding #6: Improvements needed to LDRPS access.
DTMB agrees with the recommendation and will work with State agencies to grant and maintain appropriate access to the DRPs stored in LDRPS. DTMB, working with State agencies, has already identified and granted access to all application and hardware DRPs in LDRPS. DTMB is working with State agencies to review the DR plans for content and validity which includes communicating with plan builders on areas needing improvement. DTMB will implement a periodic review of DR/BCP access. DTMB will comply with the recommendation by October 1, 2017.

Finding #7: Improved storage of DRPs and BCPs needed.
DTMB agrees with and has complied with the recommendation. DTMB's IT Continuity of Business Planning Standard 1340.070.002, as of November 2016, now states that all plans, regardless of where of the applications are housed, must be stored in the State's central repository and hardcopy backup versions of the plans are also required. DTMB is working with State agencies to ensure DRPs and BCPs utilize LDRPS as the State's central repository. Currently, all systems identified as critical are stored in the State's LDRPS.

Finding #8: Improved version control needed.
DTMB agrees with and has complied with the recommendation. DTMB work with State agencies to ensure DRPs and BCPs utilize LDRPS, as the State's central repository, which will enforce version control for DRPs and BCPs. DTMB's IT Continuity of Business Planning Standard 1340.070.002 was revised in November 2016 and now requires that all plans, regardless of where of the applications are housed, must be stored in the State's central repository. Currently, all systems identified as critical are stored in the State's LDRPS. In addition, LDRPS provides each plan with a timestamp recording the "time of last update" for version control.