Office of the Auditor General

Performance Audit Report

Executive Order No. 2016-24 Enterprise Information Management

Department of Technology, Management, and Budget

December 2018

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

071-1595-18

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
Executive Order (EO) No. 2016-24 Enterprise Information Management (EIM) Department of Technology, Management, and Budget (DTMB)

Report Number:
071-1595-18

Released:
December 2018

EO 2016-24, issued in December 2016, gave DTMB primary responsibility for implementing the EIM program throughout the State of Michigan. The EO calls for an EIM Steering Committee to provide oversight and direction of EIM program coordination and implementation within State government. The EO promotes the sharing of information while also recognizing the importance of privacy rights of confidential information.

Audit Objective			Conclusion
Objective #1: To assess the effectiveness of DTMB's efforts to comply with EO 2016-24.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DTMB did not fully implement required elements of the EO, including a centralized information sharing and analytics service center and the technologies that it will support. Only 2 (11%) of the 18 State departments had implemented the business glossary and the data sharing agreement repository and 4 (22%) of the 18 State departments had implemented or planned to implement identity master. None of the departments had implemented location master (Finding #1).		X	Agrees
DTMB should continue to develop comprehensive plans that identify the necessary resources in order to assess whether to fully implement the Statewide EIM program in accordance with EO 2016-24 (Finding #2).		X	Agrees
DTMB should further ensure that the EIM Steering Committee carries out its advisory and oversight functions regarding information security and privacy protection, as required by EO 2016-24 (Finding #3).		X	Agrees

Observations Related to this Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB should continue to communicate the roles and responsibilities of the State's Chief Data Stewards and Information Privacy Protection Officers to help ensure consistent performance of job responsibilities across all departments (Observation #1).	Not applicable for observations.		

Audit Objective	Conclusion
Objective #2: To provide a status of the State's compliance with EO 2016-24.	Status provided

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
None reported.	Not applicable.		

Exhibits Related to This Audit Objective
Exhibit #2 - Status of the State's Compliance With Executive Order No. 2016-24 Exhibit #3 - Survey Response Summary

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

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

Doug A. Ringler, CPA, CIA
Auditor General

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

December 28, 2018

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

Dear Mr. DeVries:

This is our performance audit report on Executive Order No. 2016-24, Enterprise Information Management, 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 to 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

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

EXECUTIVE ORDER NO. 2016-24

ENTERPRISE INFORMATION MANAGEMENT

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

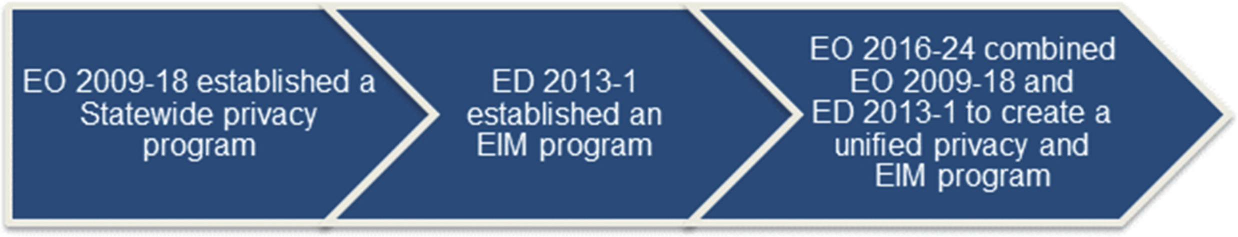
EFFORTS TO COMPLY WITH EO 2016-24

BACKGROUND

Executive Order (EO) No. 2016-24 took effect on December 21, 2016 (Exhibit #1). The EO gave the Department of Technology, Management, and Budget (DTMB) primary responsibility for the implementation of an Enterprise Information Management (EIM) program throughout the State of Michigan. The projects and goals* of the EIM program include establishment of a single Internet sign-on, improved quality of data and service delivery, and cross-agency data sharing. EO 2016-24 combined EO 2009-18, which created a Statewide privacy program, and Executive Directive (ED) No. 2013-1, which initially established an EIM program. EO 2016-24 requires the creation of a steering committee to oversee and coordinate the EIM program. The EO also requires that each State department establish a Departmental Information Management Governance Board * (DIMGB) and designate a Chief Data Steward (CDS).

In addition, the EO requires the establishment of a centralized information sharing and analytics service center, which will promote and support various EIM technologies, including:

- Business glossary - A uniform framework for business terms, data elements, and definitions.
- Data sharing agreement (DSA) repository - A collection of all DSAs that State agencies can search to determine if particular data is available to be shared.
- Identity master - An enterprise solution focused on master data and identity management.
- Location master - A centralized service for location data that State agencies can use to verify locations of citizens and businesses.



EO 2009-18 established a Statewide privacy program

ED 2013-1 established an EIM program

EO 2016-24 combined EO 2009-18 and ED 2013-1 to create a unified privacy and EIM program

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

AUDIT OBJECTIVE

To assess the effectiveness* of DTMB's efforts to comply with EO 2016-24.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DTMB appointed a Chief Data Officer (CDO) as of January 2017.
- All 18 State departments had designated a CDS and an Information Privacy Protection Officer (IPPO).
- DTMB established the EIM Steering Committee*, which meets monthly.
- DTMB incorporated EIM practices into the State Unified Information Technology Environment* (SUITE) project management and system development life cycle process.
- Single Internet sign-on had been implemented for 186 systems as of June 2018.
- DTMB and the EIM Steering Committee appropriately identified technology solutions for implementing the business glossary, DSA repository, identity master, and location master.
- DTMB made data metrics available to the public through the Open Michigan Web site and posted information related to public safety, education, public health, and economic growth.
- Three reportable conditions* related to implementation of a centralized information sharing and analytics service center; need for additional planning to assess whether to fully implement the Statewide EIM program; and need for additional EIM Steering Committee oversight (Findings #1 through #3).
- Observation* related to continued communication of roles and responsibilities (Observation #1).

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

FINDING #1

Implementation of a centralized information sharing and analytics service center needed.

DTMB did not fully implement a centralized information sharing and analytics service center and the technologies required by EO 2016-24, section I.B.4.

The benefits of a service center identified by DTMB include:

- Cost savings through the sharing and analyzing of data across State departments.
- Dedicated staff who will provide technology support across State government, leading to a more efficient use of government resources.
- More effective program management through training and support of departments in basic and advanced analytics.
- Improved program effectiveness and efficiency* through increased data sharing and analytics.
- Development of policies and processes based on data-driven decisions.

We reviewed the implementation status of the centralized information sharing and analytics service center technologies and noted:

a. Only 2 (11%) of the 18 State departments had begun implementing the business glossary technology.

   Our survey of the 18 State departments disclosed that 7 (39%) were not planning to implement the business glossary, 2 (11%) were unsure whether they would participate in the use of the business glossary, and 2 (11%) were unaware of what the business glossary was. The remaining 7 (39%) departments plan to implement the business glossary. The reasons cited by the departments for not implementing the business glossary included:

Reason for Not Implementing	Number of Departments That Cited the Reason
Low perceived value	5 (28%)
Competing priorities	4 (22%)
Lack of funding	3 (17%)
Difficulty in integrating systems	1 (6%)

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

The business glossary will help identify, define, and standardize business terms and data elements. Without a business glossary, the business terminology will vary, making it more difficult for departments to share data and hinder the capability to query, view, report, and print based on keywords. The business glossary provides a graphical view of where data originated and to which tables the data is linked, which may reduce the time and effort involved in conducting impact analyses of potential data changes.

b. Only 2 (11%) of the 18 State departments implemented the DSA repository and fully uploaded their DSAs. Four of the 18 departments were in the process of uploading DSAs.

Our survey of the 18 State departments disclosed that 3 (17%) would not participate in the use of the DSA repository, 1 (6%) was unsure whether it would participate in the DSA repository, and 1 (6%) did not know what a DSA repository was. An additional 7 (39%) departments planned to participate, but had not uploaded their DSAs to the repository. The reasons cited for not implementing the DSA repository included low perceived value and competing priorities.

The repository contains DSAs that will enable State departments to do a keyword search for existing DSAs in order to share data and result in significant time savings by joining an existing DSA rather than initiating a new one. Without a fully implemented DSA repository, departments may be unaware of what data is available and could miss out on opportunities to obtain pertinent data that is available and already being shared with other departments.

DTMB informed us that the DSA repository was implemented in February 2017. The EIM Steering Committee officially adopted SharePoint as the DSA platform in November 2017. DTMB established a goal of 100% participation by September 30, 2018.

c. DTMB did not fully implement identity master technology. Identity master originated in the Michigan Department of Health and Human Services, and DTMB planned to make the technology available to all State departments by fiscal year 2019.

However, our survey of the 18 State departments disclosed that 4 (22%) did not plan to implement identity master, 8 (44%) were unsure if they would implement it, and 2 (11%) were unaware of what it was. The remaining 4 (22%) departments planned to implement identity master. The reason cited for not doing so was a low perceived value.

Identity master technology will allow State departments to instantly determine the accuracy of information used to identify individuals by cross-referencing to a single most reliable source of identity information. Identity master uniquely identifies an individual based on his/her interactions with various State departments by using information such as student, driver, voter, taxpayer, lottery winner, beneficiary, and claimant data. Without Statewide implementation, departments may use inaccurate identity information when matching data from multiple systems.

d. None of the 18 State departments had implemented the location master technology.

Statewide implementation was on hold and removed from the EIM Steering Committee's goals because of the low perceived value and lack of funding by the State departments.

Location master is a centralized service to standardize and validate address and geographical data. Location master helps support mail delivery to proper addresses and assists in identifying boundaries such as school districts and voting precincts. Location data will be verified by cross-referencing to a single most reliable source of geographic information. For example, the base map can be used for department-specific items of interest, including roads; culverts; railroads; trails; recreation and hunting areas; oil and gas fields; wells; schools; and licensed facilities such as foster care, child care, and health care.

RECOMMENDATION

We recommend that DTMB fully implement a centralized information sharing and analytics service center and the technologies required by EO 2016-24.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation.

DTMB has implemented components of the Analytics Service Center (ASC), and the EIM Steering Committee endorsed a conceptual vision of the ASC at their September 4, 2018 meeting. Implementation of that vision is in progress.

DTMB has implemented the IT infrastructure, tools, and enterprise service capability for business glossary, DSA repository, identity master, location master, as well as components of the ASC such as a reporting/analytics service and self-service data visualization. Onboarding agencies to these solutions is an ongoing activity.

Since completion of the Office of the Auditor General (OAG) field work in August 2018, DTMB has demonstrated progress in the following areas:

- *Identity master: Additional and more detailed analysis of transitioning the Michigan Department of Health and Human Services (MDHHS) identity master solution to DTMB as an enterprise service identified unacceptable complexity, risk, and cost. Alternatively, DTMB and the EIM Steering Committee decided to leverage the existing DTMB Master Data Management (MDM) technology platform as an enterprise identity master solution, incorporating the MDHHS solution as a data source. The DTMB platform is already funded as an enterprise rated service. Work is in progress with the first agency customer to use the new enterprise identity master service.*

- *Location master: The November 2018 technology upgrade of the Michigan Geographic Framework (MGF) meets the requirements of location master and is already funded as an enterprise rated service. Current customers of the master data management solution for location include the Michigan Department of Transportation (MDOT), Department of Natural Resources (DNR), and the 21st Century Infrastructure Commission.*

FINDING #2

Additional planning needed to fully implement the Statewide EIM program.

DTMB should continue to develop comprehensive plans that identify the necessary resources in order to assess whether to fully implement the Statewide EIM program in accordance with EO 2016-24.

DTMB, in conjunction with State departments, should:

a. Fully identify the systems, by department, in which key data resides.

   Instead, DTMB created a data inventory that identified the types of data that each department owns. Knowing where data resides is critical to integrating with EIM technologies and will enable DTMB to make informed decisions when determining the systems to integrate within the EIM program to provide the greatest benefit to the State. Also, DTMB may be unable to determine the total cost of integrating the selected systems within the EIM program, as discussed in part b. of this finding.

   Control Objectives for Information and Related Technology* (COBIT) states that management should create and maintain an inventory of information systems and data, including system owners, custodians, and classifications.

b. Identify the resources needed to achieve full implementation and continued operation of the EIM program, such as the number of personnel and amount of funding needed at the department and enterprise levels.

   DTMB established a rate structure for all technologies, except identity master. Part of the implementation cost is determined by multiplying the rate structure by the number of systems to be integrated. However, until all systems to be integrated are identified, as described in part a. of this finding, the total cost of implementing the EIM program cannot be determined and DTMB cannot collaborate with State departments to seek funding.

   DTMB submitted proposals for change to the State Budget Office to request funding for EIM program implementation and received a total of $5.1 million for fiscal years 2015 and 2016 and $1.3 million for fiscal year 2018, which was significantly less than the $7.5 million requested for fiscal year 2018. Because the proposals for change did not include a complete analysis of the funding needed for Statewide implementation, the full benefits of the EIM program may not be realized.

   COBIT 5 APO02.05 recommends that management identify and adequately address costs and staffing in the

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

planning process. DTMB's SUITE Project Management Methodology Manual also requires that the project planning phase address all aspects of project management and include items such as time, cost, and human resources.

c. Set target implementation dates for the EIM program, by department, for the systems determined in part a. and the resources determined in part b. of this finding.

Setting target dates would allow departments to better prioritize resources, develop realistic implementation plans, and give DTMB the ability to hold departments accountable for missed deadlines.

DTMB contracted with PricewaterhouseCoopers (PwC) to assist in the implementation of the EIM program. One of the deliverables was to develop roadmaps for each State department that would provide a high-level overview of critical EIM components. PwC presented the roadmaps to DTMB and all agencies in December 2015 and January 2016. Although the roadmaps were intended to be at a high level, as of July 2018, DTMB had not expanded upon them to include the systems to be integrated, costs, and target implementation dates.

We surveyed 47 CDSs and IPPOs from the 18 State departments and received responses from 39 individuals. Their responses indicated the following challenges to full implementation of the required technologies:

Challenge to Full Implementation	Number of Departments
Conflicting priorities	17 (94%)
Lack of funding	13 (72%)
Lack of staffing	12 (67%)
Other	10 (56%)
Lack of leadership such as executive sponsorship	3 (17%)
No challenges to full implementation	1 (6%)

RECOMMENDATION

We recommend that DTMB continue to develop comprehensive plans that identify the necessary resources in order to assess whether to fully implement the Statewide EIM program in accordance with EO 2016-24.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation.

Not all department systems and data are required to implement all components of the EIM program. Only those systems and data that present a positive business case from the department and enterprise perspective are relevant. Additionally, the Statewide data inventory is intentionally data centric and does include the system in which the data resides. DTMB has created and maintains similar inventories that focus on cyber security/risk mitigation and infrastructure components. These combined inventories provide a comprehensive view of State of Michigan (SOM) systems.

DTMB will continue to refine its implementation plans to realize the vision articulated in EO 2016-24. Since completion of the OAG field work in August 2018, DTMB has demonstrated progress in the following areas:

- *As noted in Finding #1, DTMB Enterprise Services will provide the identity master solution and a rated service cost model already exists for the technology platform.*

- *EIM and data considerations were incorporated in the SUITE framework in December 2018. Based on industry best practices, SUITE is the State of Michigan's framework for project/portfolio management and systems engineering. The addition of EIM to this Statewide framework will improve project planning and project management by addressing topics such as time, cost, human resources, decisions on buy/build/share, benefits realization, and total cost of ownership.*

DTMB and the EIM Steering Committee will continue to request funding for the EIM program.

FINDING #3

Additional EIM Steering Committee oversight needed.

DTMB should further ensure that the EIM Steering Committee carries out its advisory and oversight functions regarding information security* and privacy protection, as required by EO 2016-24. Without oversight, the State may be unable to address challenges to EO implementation in a timely fashion and may not achieve full compliance with the EO.

The Steering Committee performed 2 of the 5 responsibilities required by EO 2016-24, part L., including (1) recommending strategies to enhance awareness, education, and understanding of information security best practices and online measures to protect personally identifiable information* (PII) and (2) recommending training programs for State employees regarding information security and privacy protection.

To further accomplish its advisory and oversight functions, the Steering Committee should:

a. Review and monitor each State department's implementation of its privacy framework and corresponding department policies and procedures to ensure compliance with privacy laws.

   Our survey of the 18 State departments indicated that all departments had selected a privacy framework as required by DTMB Administrative Guide procedure 2600.01; however, 14 had not implemented the framework. Time frames to implement the selected frameworks ranged from 6 to 36 months. DTMB Administrative Guide procedure 2600.01 states that departments have until May 15, 2019 to adopt a privacy framework and develop an implementation plan. The time frame for achieving a fully defined and managed privacy program will be in accordance with each department's implementation plan. As a result, privacy policy and procedure implementation will vary by department and could be untimely and inconsistent.

b. Fully develop and implement a process, in conjunction with DTMB's Michigan Cybersecurity Division (MCS), to identify information security and privacy protection risks within State government and recommend risk mitigation strategies, methods, and procedures to be adopted by State departments and agencies to mitigate these risks.

In August 2018, subsequent to bringing this matter to management's attention, the Steering Committee approved a process to expand the Privacy Workgroup to include all IPPOs who will review, discuss, and monitor department privacy implementation plans and semiannually report to the Steering Committee on the status of compliance. Also, the Steering Committee adopted an annual reporting process by MCS that will

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

identify security risks and provide risk mitigation strategies and recommendations.

RECOMMENDATION

We recommend that DTMB further ensure that the EIM Steering Committee carries out its advisory and oversight functions regarding information security and privacy protection, as required by EO 2016-24.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation.

Since EO 2016-24 was enacted, DTMB and the EIM Steering Committee have been executing required advisory and appropriate oversight functions regarding security and privacy protection.

In addition to ongoing advisory and oversight functions, the Steering Committee has identified the following activities:

- *Additional enterprise-wide privacy procedures are in the final review process and will be placed in the Administrative Guide.*

- *DTMB and the EIM Steering Committee will continue to assist departments in achieving a defined and managed privacy program, including ensuring appropriate implementation timelines.*

- *DTMB already has a strong information security function. The DTMB Office of Cybersecurity and Infrastructure Protection is scheduled to provide a briefing to the EIM Steering Committee twice annually.*

OBSERVATION #1

Continued communication of roles and responsibilities needed.

DTMB should continue to communicate the roles and responsibilities of the State's CDSs and IPPOs to help ensure consistent performance of job responsibilities across all departments.

The CDS and IPPO roles are critical to the successful implementation of the State's EIM program and to achieve the vision of the EO. These roles include duties such as advising the DIMGB on Statewide EIM activities; coordinating privacy law compliance; implementing EIM within the departments; creating and reviewing departmental privacy policies, standards, and procedures; and performing departmental privacy risk assessment, compliance monitoring, and remediation activities.

In February 2015, DTMB provided training to CDSs regarding the concepts of an information management program and the State's direction and activities for its EIM program. This training also included some aspects of the roles and responsibilities of a CDS and an IPPO. However, 22 (61%) of 36 individuals responding to our survey had served in the CDS or IPPO role for less than 2 years and would not have attended the training.

In August 2017, DTMB distributed a list of key IPPO duties to all department deputy directors asking for language to be included in the IPPOs' position descriptions.

DTMB could further communicate CDS and IPPO roles by actions such as enhancing training and intranet materials, developing an onboarding program for individuals who are new to these roles, enhancing policies and procedures, or including the roles and responsibilities in performance evaluations or position descriptions.

Additional training and communication of roles and responsibilities would help ensure that all CDSs and IPPOs understand the direction and goals of the EIM Steering Committee and consistently perform their job responsibilities to successfully implement EO 2016-24.

STATUS OF COMPLIANCE WITH EO 2016-24

BACKGROUND

EO 2016-24 was created in December 2016, replacing ED 2013-1 and EO 2009-18. EO 2016-24 provided for a Statewide EIM and privacy program coordinated through DTMB.

AUDIT OBJECTIVE

To provide a status of the State's compliance with EO 2016-24.

CONCLUSION

Status provided.

FACTORS IMPACTING CONCLUSION

- Exhibit #2 presents the OAG's determination of the compliance status of selected elements of EO 2016-24.

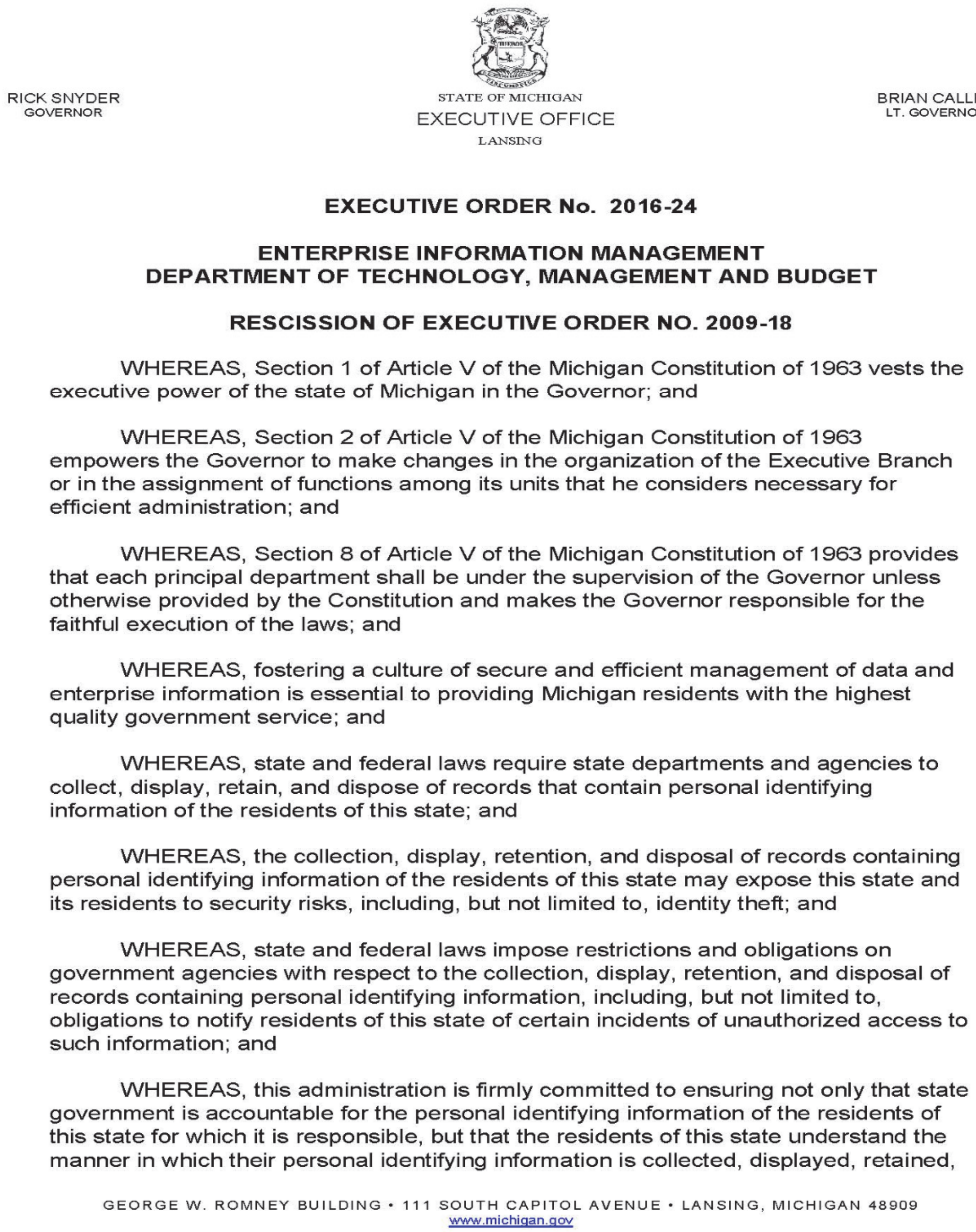
- Exhibit #3 presents a summary of selected survey questions and responses by the 18 State departments.

SUPPLEMENTAL INFORMATION

Exhibit #1

EXECUTIVE ORDER NO. 2016-24
Department of Technology, Management, and Budget

Executive Order No. 2016-24
Effective Date: December 21, 2016



RICK SNYDER
GOVERNOR

STATE OF MICHIGAN
EXECUTIVE OFFICE
LANSING

BRIAN CALLEY
LT. GOVERNOR

EXECUTIVE ORDER No. 2016-24

ENTERPRISE INFORMATION MANAGEMENT
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET

RESCISSION OF EXECUTIVE ORDER NO. 2009-18

WHEREAS, Section 1 of Article V of the Michigan Constitution of 1963 vests the executive power of the state of Michigan in the Governor; and

WHEREAS, Section 2 of Article V of the Michigan Constitution of 1963 empowers the Governor to make changes in the organization of the Executive Branch or in the assignment of functions among its units that he considers necessary for efficient administration; and

WHEREAS, Section 8 of Article V of the Michigan Constitution of 1963 provides that each principal department shall be under the supervision of the Governor unless otherwise provided by the Constitution and makes the Governor responsible for the faithful execution of the laws; and

WHEREAS, fostering a culture of secure and efficient management of data and enterprise information is essential to providing Michigan residents with the highest quality government service; and

WHEREAS, state and federal laws require state departments and agencies to collect, display, retain, and dispose of records that contain personal identifying information of the residents of this state; and

WHEREAS, the collection, display, retention, and disposal of records containing personal identifying information of the residents of this state may expose this state and its residents to security risks, including, but not limited to, identity theft; and

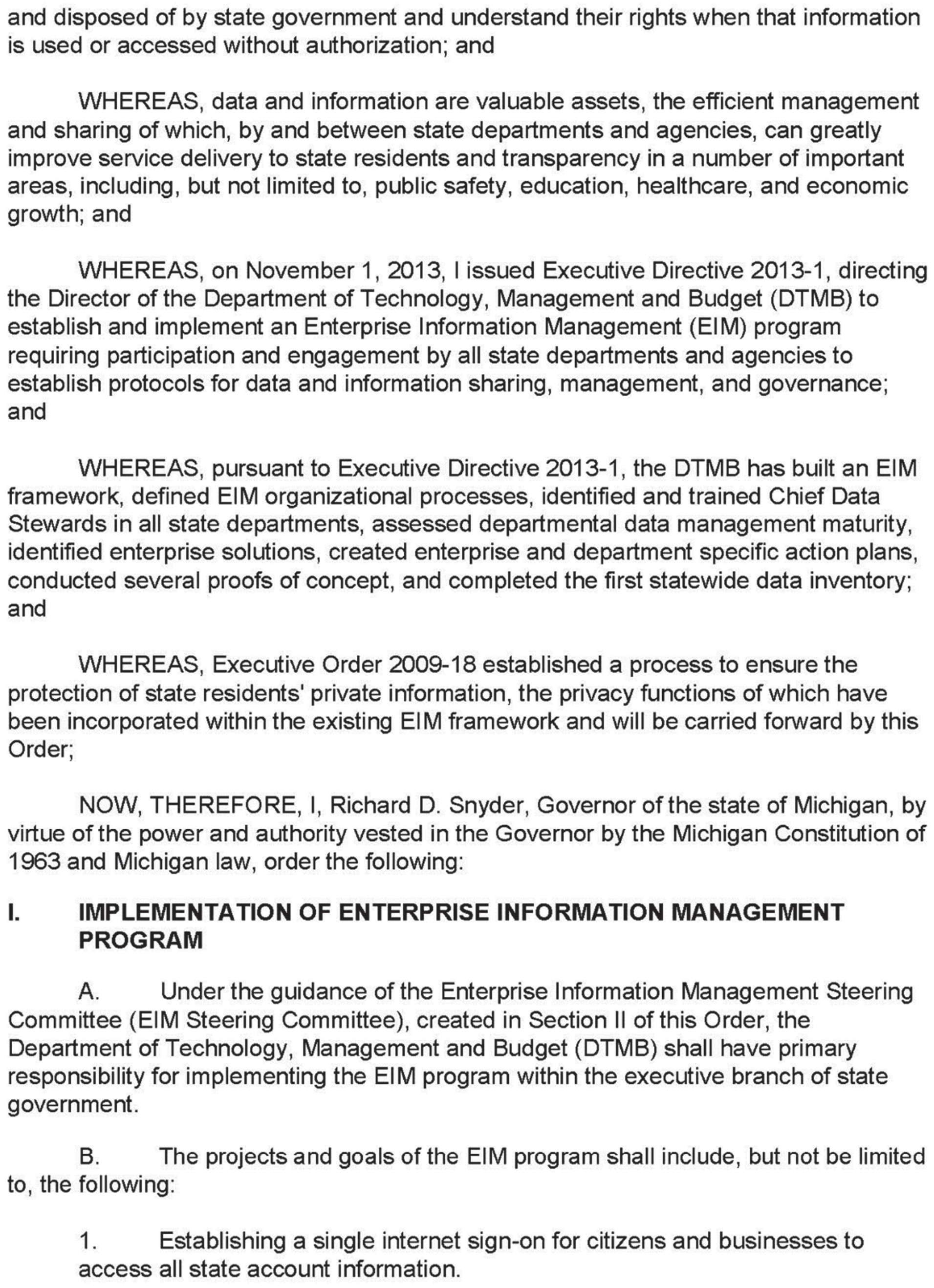
WHEREAS, state and federal laws impose restrictions and obligations on government agencies with respect to the collection, display, retention, and disposal of records containing personal identifying information, including, but not limited to, obligations to notify residents of this state of certain incidents of unauthorized access to such information; and

WHEREAS, this administration is firmly committed to ensuring not only that state government is accountable for the personal identifying information of the residents of this state for which it is responsible, but that the residents of this state understand the manner in which their personal identifying information is collected, displayed, retained,

GEORGE W. ROMNEY BUILDING • 111 SOUTH CAPITOL AVENUE • LANSING, MICHIGAN 48909
www.michigan.gov

This exhibit continued on next page.

Exhibit #1
(Continued)



and disposed of by state government and understand their rights when that information is used or accessed without authorization; and

WHEREAS, data and information are valuable assets, the efficient management and sharing of which, by and between state departments and agencies, can greatly improve service delivery to state residents and transparency in a number of important areas, including, but not limited to, public safety, education, healthcare, and economic growth; and

WHEREAS, on November 1, 2013, I issued Executive Directive 2013-1, directing the Director of the Department of Technology, Management and Budget (DTMB) to establish and implement an Enterprise Information Management (EIM) program requiring participation and engagement by all state departments and agencies to establish protocols for data and information sharing, management, and governance; and

WHEREAS, pursuant to Executive Directive 2013-1, the DTMB has built an EIM framework, defined EIM organizational processes, identified and trained Chief Data Stewards in all state departments, assessed departmental data management maturity, identified enterprise solutions, created enterprise and department specific action plans, conducted several proofs of concept, and completed the first statewide data inventory; and

WHEREAS, Executive Order 2009-18 established a process to ensure the protection of state residents' private information, the privacy functions of which have been incorporated within the existing EIM framework and will be carried forward by this Order;

NOW, THEREFORE, I, Richard D. Snyder, Governor of the state of Michigan, by virtue of the power and authority vested in the Governor by the Michigan Constitution of 1963 and Michigan law, order the following:

I. IMPLEMENTATION OF ENTERPRISE INFORMATION MANAGEMENT PROGRAM

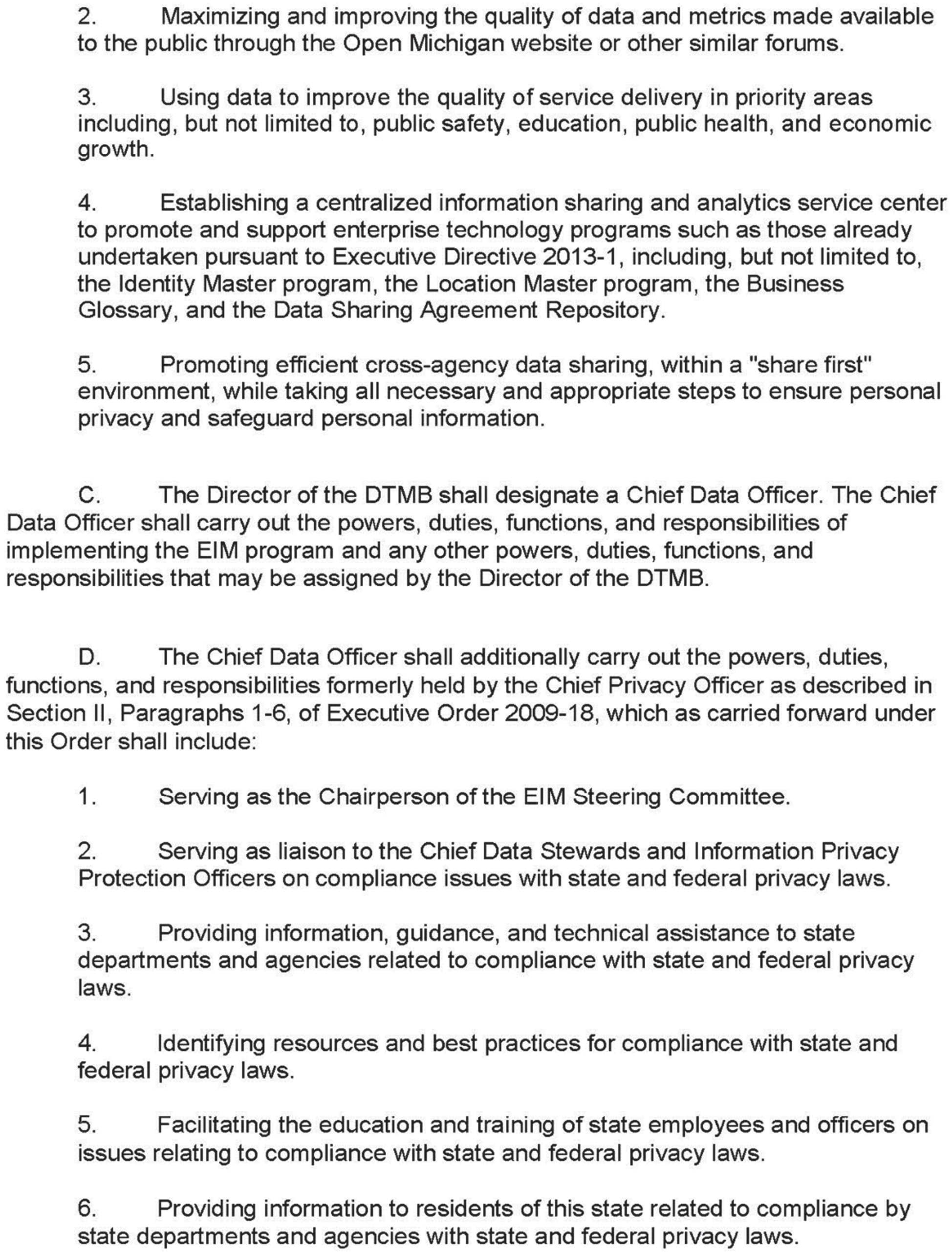
A. Under the guidance of the Enterprise Information Management Steering Committee (EIM Steering Committee), created in Section II of this Order, the Department of Technology, Management and Budget (DTMB) shall have primary responsibility for implementing the EIM program within the executive branch of state government.

B. The projects and goals of the EIM program shall include, but not be limited to, the following:

1. Establishing a single internet sign-on for citizens and businesses to access all state account information.

This exhibit continued on next page.

Exhibit #1
(Continued)



2. Maximizing and improving the quality of data and metrics made available to the public through the Open Michigan website or other similar forums.

3. Using data to improve the quality of service delivery in priority areas including, but not limited to, public safety, education, public health, and economic growth.

4. Establishing a centralized information sharing and analytics service center to promote and support enterprise technology programs such as those already undertaken pursuant to Executive Directive 2013-1, including, but not limited to, the Identity Master program, the Location Master program, the Business Glossary, and the Data Sharing Agreement Repository.

5. Promoting efficient cross-agency data sharing, within a "share first" environment, while taking all necessary and appropriate steps to ensure personal privacy and safeguard personal information.

C. The Director of the DTMB shall designate a Chief Data Officer. The Chief Data Officer shall carry out the powers, duties, functions, and responsibilities of implementing the EIM program and any other powers, duties, functions, and responsibilities that may be assigned by the Director of the DTMB.

D. The Chief Data Officer shall additionally carry out the powers, duties, functions, and responsibilities formerly held by the Chief Privacy Officer as described in Section II, Paragraphs 1-6, of Executive Order 2009-18, which as carried forward under this Order shall include:

1. Serving as the Chairperson of the EIM Steering Committee.

2. Serving as liaison to the Chief Data Stewards and Information Privacy Protection Officers on compliance issues with state and federal privacy laws.

3. Providing information, guidance, and technical assistance to state departments and agencies related to compliance with state and federal privacy laws.

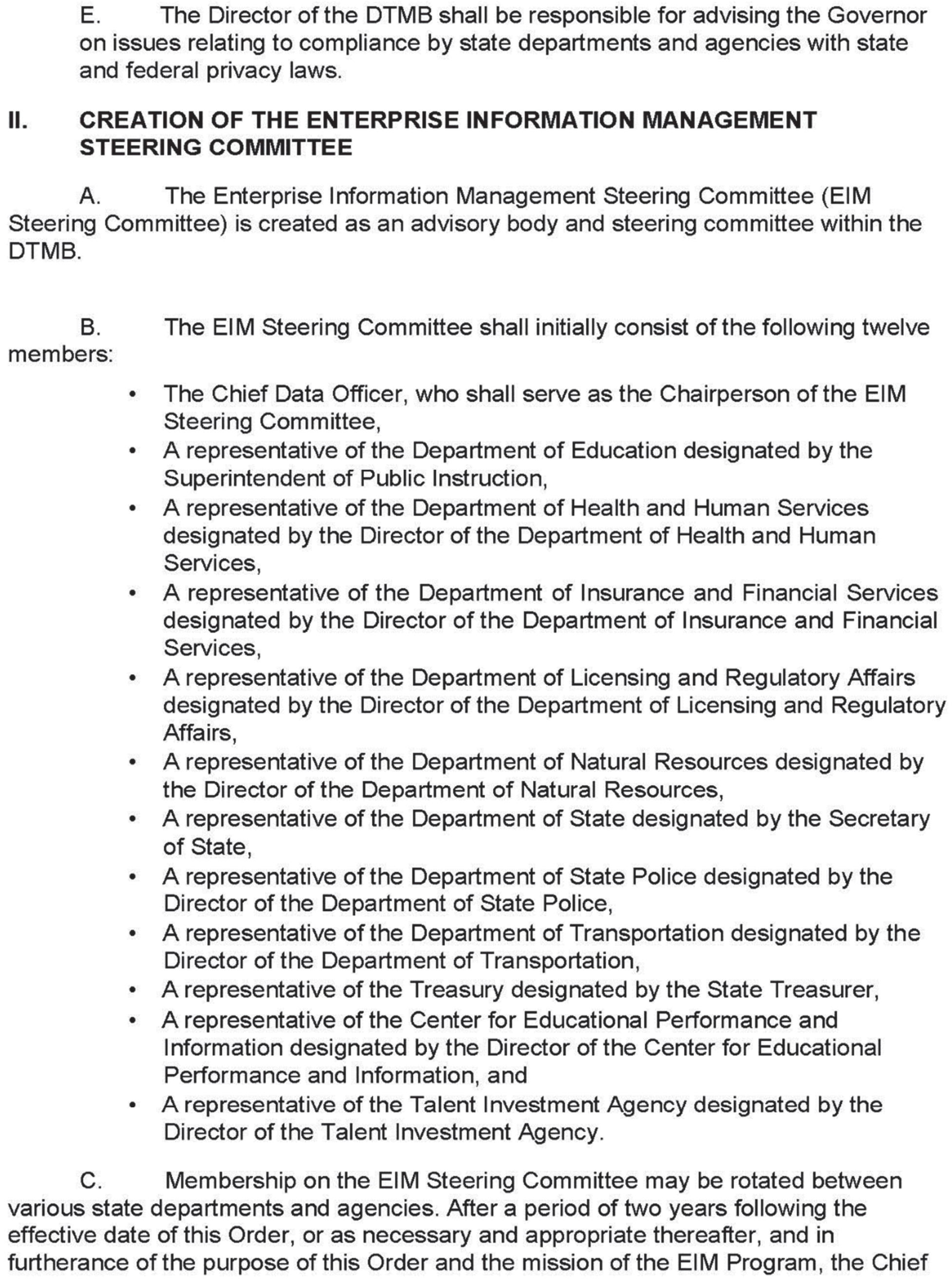
4. Identifying resources and best practices for compliance with state and federal privacy laws.

5. Facilitating the education and training of state employees and officers on issues relating to compliance with state and federal privacy laws.

6. Providing information to residents of this state related to compliance by state departments and agencies with state and federal privacy laws.

This exhibit continued on next page.

Exhibit #1
(Continued)



E. The Director of the DTMB shall be responsible for advising the Governor on issues relating to compliance by state departments and agencies with state and federal privacy laws.

II. CREATION OF THE ENTERPRISE INFORMATION MANAGEMENT STEERING COMMITTEE

A. The Enterprise Information Management Steering Committee (EIM Steering Committee) is created as an advisory body and steering committee within the DTMB.

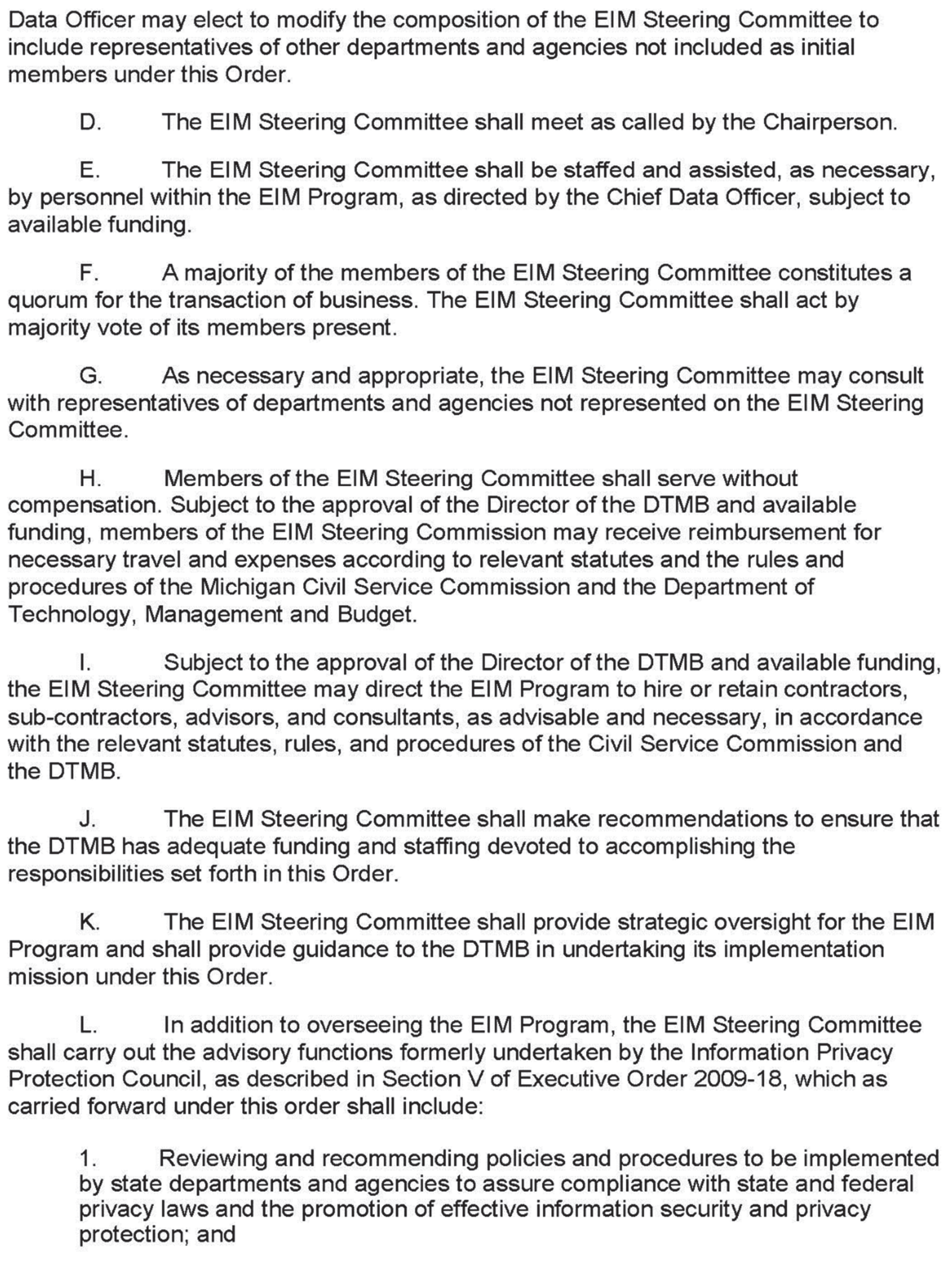
B. The EIM Steering Committee shall initially consist of the following twelve members:

- The Chief Data Officer, who shall serve as the Chairperson of the EIM Steering Committee,
- A representative of the Department of Education designated by the Superintendent of Public Instruction,
- A representative of the Department of Health and Human Services designated by the Director of the Department of Health and Human Services,
- A representative of the Department of Insurance and Financial Services designated by the Director of the Department of Insurance and Financial Services,
- A representative of the Department of Licensing and Regulatory Affairs designated by the Director of the Department of Licensing and Regulatory Affairs,
- A representative of the Department of Natural Resources designated by the Director of the Department of Natural Resources,
- A representative of the Department of State designated by the Secretary of State,
- A representative of the Department of State Police designated by the Director of the Department of State Police,
- A representative of the Department of Transportation designated by the Director of the Department of Transportation,
- A representative of the Treasury designated by the State Treasurer,
- A representative of the Center for Educational Performance and Information designated by the Director of the Center for Educational Performance and Information, and
- A representative of the Talent Investment Agency designated by the Director of the Talent Investment Agency.

C. Membership on the EIM Steering Committee may be rotated between various state departments and agencies. After a period of two years following the effective date of this Order, or as necessary and appropriate thereafter, and in furtherance of the purpose of this Order and the mission of the EIM Program, the Chief

This exhibit continued on next page.

Exhibit #1
(Continued)



Data Officer may elect to modify the composition of the EIM Steering Committee to include representatives of other departments and agencies not included as initial members under this Order.

D. The EIM Steering Committee shall meet as called by the Chairperson.

E. The EIM Steering Committee shall be staffed and assisted, as necessary, by personnel within the EIM Program, as directed by the Chief Data Officer, subject to available funding.

F. A majority of the members of the EIM Steering Committee constitutes a quorum for the transaction of business. The EIM Steering Committee shall act by majority vote of its members present.

G. As necessary and appropriate, the EIM Steering Committee may consult with representatives of departments and agencies not represented on the EIM Steering Committee.

H. Members of the EIM Steering Committee shall serve without compensation. Subject to the approval of the Director of the DTMB and available funding, members of the EIM Steering Commission may receive reimbursement for necessary travel and expenses according to relevant statutes and the rules and procedures of the Michigan Civil Service Commission and the Department of Technology, Management and Budget.

I. Subject to the approval of the Director of the DTMB and available funding, the EIM Steering Committee may direct the EIM Program to hire or retain contractors, sub-contractors, advisors, and consultants, as advisable and necessary, in accordance with the relevant statutes, rules, and procedures of the Civil Service Commission and the DTMB.

J. The EIM Steering Committee shall make recommendations to ensure that the DTMB has adequate funding and staffing devoted to accomplishing the responsibilities set forth in this Order.

K. The EIM Steering Committee shall provide strategic oversight for the EIM Program and shall provide guidance to the DTMB in undertaking its implementation mission under this Order.

L. In addition to overseeing the EIM Program, the EIM Steering Committee shall carry out the advisory functions formerly undertaken by the Information Privacy Protection Council, as described in Section V of Executive Order 2009-18, which as carried forward under this order shall include:

1. Reviewing and recommending policies and procedures to be implemented by state departments and agencies to assure compliance with state and federal privacy laws and the promotion of effective information security and privacy protection; and

This exhibit continued on next page.

Exhibit #1
(Continued)

2. Recommending strategies to enhance awareness, education, and understanding of information security best practices and online measures intended to protect the personal identifiable information of residents of this state; and

3. Identifying information security and privacy protection risks within state government and recommending risk mitigation strategies, methods, and procedures to be adopted by state departments and agencies to lessen these risks; and

4. Monitoring compliance by state departments and agencies with state information security and privacy protection policies and procedures; and

5. Recommending training programs for state employees designed to educate, promote, and advance knowledge of information security and privacy protection procedures.

III. INFORMATION MANAGEMENT GOVERNANCE BOARDS

A. Each principal department director shall create and establish a Departmental Information Management Governance Board (DIMGB) to provide an operational support structure for and to coordinate with the EIM Steering Committee.

B. The DIMGB within each principal department shall be chaired by the department director or chief deputy director, include the Chief Data Steward and Privacy Protection Officer identified as provided in Section IV of this Order, and shall have membership representation from all bureau or division administrators that have responsibility over business data or information management systems.

C. The DIMGB within each principal department shall advise, adopt, and support all activities related to achieving the goals of secure and efficient enterprise information management within each department and agency.

IV. CHIEF DATA STEWARDS AND PRIVACY PROTECTION OFFICERS

A. Each principal department shall designate a Chief Data Steward responsible for implementing secure and efficient enterprise information management within each department and agency who shall provide administrative support to the DIMGB within each principal department.

B. Each principal department shall designate an Information Privacy Protection Officer as the primary coordinator of departmental compliance with state and federal privacy laws, and as an advisor to the DIMGB on best practices for enterprise-wide privacy and security matters. The Chief Data Steward may be the Privacy Protection Officer.

This exhibit continued on next page.

Exhibit #1
(Continued)

C. The Chief Data Steward and Information Privacy Protection Officer within each principal department shall cooperate and coordinate with the Chief Data Officer or their designee on compliance issues with state and federal privacy laws.

D. Each principal department shall ensure that sufficient funding and staffing are devoted to support the Chief Data Stewards' performance of the functions required by this Order.

V. RESCISSION OF EXECUTIVE ORDER 2009-18

A. The position of Chief Privacy Officer created by Executive Order 2009-18 is abolished.

B. The Information Privacy Protection Council created by Executive Order 2009-18 is abolished.

C. Executive Order 2009-18 is rescinded in its entirety.

VI. MISCELLANEOUS

A. Any suit, action, or other proceeding lawfully commenced by, against, or before any entity affected under this Order shall not abate by any reason or by the taking effect of this Order.

B. Nothing in this Order shall be construed to change the organization of the executive branch of state government or the assignment of functions among its units in a manner requiring the force of law.

C. The invalidity of any portion of this Order shall not affect the validity of the remainder of the Order, which may be given effect without any invalid portion.

The Executive Order shall become effective upon filing.

Given under my hand and the Great Seal of the state of Michigan this 21st day of December, in the year of our Lord, Two Thousand Sixteen

(signature redacted)
RICHARD D. SNYDER
GOVERNOR

BY THE GOVERNOR:

(signature redacted)
SECRETARY OF STATE

FILED WITH SECRETARY OF STATE
ON 12/21/2016 AT 10:22am

Source: michigan.gov.

Exhibit #2

EXECUTIVE ORDER NO. 2016-24
Department of Technology, Management, and Budget

Status of the State's Compliance With Executive Order No. 2016-24
As of August 1, 2018

OAG-Determined Compliance Status	Definition of Status
Ongoing	Efforts to address the EO requirement have begun; however, continuous effort is needed to achieve or maintain compliance.
Completed	The most significant aspects of the EO requirement have been addressed.
Partially completed	Some aspects of the EO requirement have been addressed.
Not completed	The most significant aspects of the EO requirement have not been addressed.

EO Section	EO Requirement	OAG-Determined Compliance Status
I.B.1	Establish a single Internet sign-on for citizens and businesses to access all State account information.	Ongoing
I.B.2	Maximize and improve the quality of data and metrics made available to the public through the Open Michigan Web site or other similar forums.	Ongoing
I.B.3	Use data to improve the quality of service delivery in priority areas, including, but not limited to, public safety, education, public health, and economic growth.	Ongoing
I.B.4	Establish a centralized information sharing and analytics service center.	Partially completed
I.B.5	Promote efficient cross-agency data sharing within a "share first" environment.	Ongoing
I.C	The DTMB Director shall designate a CDO.	Completed
I.D.6	The CDO shall provide information to residents of this State related to compliance by State departments and agencies with State and federal privacy laws.	Not completed
I.E	The DTMB Director shall be responsible for advising the Governor on issues relating to compliance by State departments and agencies with State and federal privacy laws.	Ongoing
II.B	The EIM Steering Committee shall initially consist of twelve members, including the CDO and representatives from the following agencies: Michigan Department of Education, Michigan Department of Health and Human Services, Department of Insurance and Financial Services, Department of Licensing and Regulatory Affairs, Department of Natural Resources, Department of State, Michigan Department of State Police, Michigan Department of Transportation, Department of Treasury, Center for Educational Performance Information, and Talent Investment Agency.	Completed
II.J	The EIM Steering Committee shall make recommendations to ensure that DTMB has adequate funding and staffing devoted to accomplishing the responsibilities set forth in this EO.	Completed

This exhibit continued on next page.

Exhibit #2
(Continued)

EO Section	EO Requirement	OAG-Determined Compliance Status
II.L.1	The EIM Steering Committee shall review and recommend policies and procedures to be implemented by State departments and agencies to ensure compliance with State and federal privacy laws and the promotion of effective information security and privacy protection.	Partially completed
II.L.2	The EIM Steering Committee shall recommend strategies to enhance awareness, education, and understanding of information security best practices and online measures intended to protect the personally identifiable information of residents of this State.	Completed
II.L.3	The EIM Steering Committee shall identify information security and privacy protection risks within State government and recommend risk mitigation strategies, methods, and procedures to be adopted by State departments and agencies to lessen these risks.	Partially completed
II.L.4	The EIM Steering Committee shall monitor compliance by State departments and agencies with State information security and privacy protection policies and procedures.	Not completed*
II.L.5	The EIM Steering Committee shall recommend training programs for State employees designed to educate, promote, and advance knowledge of information security and privacy protection procedures.	Completed
III	Each department director shall create and establish a DIMGB. Each DIMGB shall be chaired by the department director or chief deputy director, include the CDS and IPPO identified, and shall have membership representation from all bureau or division administrators that have responsibility over business data or information management systems. The DIMGBs shall advise, adopt, and support all activities related to achieving the goals of a secure and efficient enterprise information management within each department and agency.	Partially completed
IV.A	Each principal department shall designate a CDS.	Completed
IV.B	Each principal department shall designate an IPPO.	Completed
IV.D	Each principal department shall ensure that sufficient funding and staffing are devoted to support the CDS's performance of the functions required by this EO.	Partially completed

* Subsequent to our fieldwork, DTMB informed us that it developed a process to monitor compliance by State departments and agencies with information security and privacy protection policies and procedures.

Source: The OAG prepared this exhibit based on EO 2016-24 and information obtained from DTMB personnel during the audit. The OAG used professional judgment to determine the status of the EO requirements.

UNAUDITED
Exhibit #3

EXECUTIVE ORDER NO. 2016-24
Department of Technology, Management, and Budget

Survey Response Summary

We sent an online survey to 47 Chief Data Stewards (CDSs) and Information Privacy Protection Officers (IPPOs) from the 18 State departments and received responses from 39 (83%) individuals. The survey focused on Executive Order (EO) No. 2016-24 implementation plans by each department. Following is a summary of selected survey results, including the number and percentage of responses received for each question. Because some departments had multiple respondents, and, depending on the nature of the question, we aggregated survey responses by department. Also, if a single respondent answered in the affirmative, we recorded in the affirmative for the department as a whole.

Q1 What is your role in the Enterprise Information Management (EIM) program, as required within EO No. 2016-24?

	Responses	
CDS	14	(36%)
IPPO	8	(21%)
Department Security Officer (DSO)	1	(3%)
CDS, IPPO, and DSO	5	(13%)
IPPO and DSO	8	(21%)
CDS and IPPO	1	(3%)
CDS and DSO	1	(3%)
None of the above	1	(3%)

Q2 Please indicate how long you have held the following roles:

	CDS	IPPO	DSO
Less than 1 year	3	5	1
1 to 2 years	7	6	3
Greater than 2 years	6	6	10

Q3 Have you received any training specific to your role as CDS or IPPO?

	CDS	IPPO
Yes	10	11
No	7	5
No response	1	2

This exhibit continued on next page.

UNAUDITED
Exhibit #3
(Continued)

Q4 Has your department assessed the risks associated with data privacy?

	Responses by Department	
Yes	13	(72%)
No	2	(11%)
I am unsure.	2	(11%)
No response	1	(6%)

Q5 Does your department share personally identifiable information (PII) such as social security numbers, dates of birth, and addresses?

	Responses by Department	
Yes	14	(78%)
No	3	(17%)
No response	1	(6%)

Q6 With whom does your department share PII (choose all that apply)?

	Responses by Department	
Other SOM departments or agencies	14	(78%)
Contracted service providers	11	(61%)
Federal government agencies	10	(56%)
Researchers	6	(33%)
Individuals when a FOIA request is received	6	(33%)
Other state governments	5	(28%)
Local governments	5	(28%)
No response	4	(22%)
Other entities	2	(11%)
Individuals when a FOIA request is not received	1	(6%)
Private businesses	1	(6%)

Q7 What safeguards are in place to protect the PII that you have shared with others (choose all that apply)? My department:

	Responses by Department	
Requires signed confidentiality agreements.	12	(67%)
Has policies and procedures for PII data sharing.	10	(56%)
Monitors third party access to the State's data.	7	(39%)
Other safeguards	4	(22%)
No response	4	(22%)

This exhibit continued on next page.

UNAUDITED
Exhibit #3
(Continued)

Q8 Please indicate the extent to which the following privacy practices are in place within your department. My department:

	Always	Sometimes	Never	No Response
Limits access to PII based on business need.	12	5	0	1
Limits electronic access to PII.	13	4	0	1
Limits physical access to PII.	13	3	1	1
Trains staff on proper handling of PII.	8	9	0	1
Monitors disposal of the PII in electronic files.	5	8	4	1
Monitors disposal of the PII in paper documents.	8	6	3	1
Allows citizens to review their own PI.I	4	10	3	1
Classifies PII (private, confidential, or public).	10	7	0	1
Corrects PII upon citizens' request.	6	11	0	1
Inventories PII.	6	10	1	1
Limits data collection to necessary PII.	8	9	0	1
Notifies citizens if their PII is disclosed.	8	8	1	1
Relies solely on DTMB for privacy practices.	2	11	4	1

Q9 Please specify the extent to which you agree with each of the following statements related to privacy practices within your department. My department has:

	Strongly Agree	Agree	No Basis for Opinion	Disagree	Strongly Disagree	No Response
Identified data requiring protection.	7	10	0	0	0	1
Policies in place to protect personal data.	6	7	2	2	0	1
Procedures in place to protect personal data.	4	10	2	1	0	1
Adequate technology available to protect data.	4	8	4	1	0	1
Expertise to protect personal data.	2	11	3	1	0	1
Adequate time to protect data.	3	7	6	1	0	1
Identified data privacy as a strategic issue.	3	10	4	0	0	1
Management that supports implementing privacy protection.	8	8	1	0	0	1
Necessary funding to implement privacy practices.	0	8	3	4	2	1
No privacy issues.	1	7	2	3	4	1

This exhibit continued on next page.

UNAUDITED
Exhibit #3
(Continued)

Q10 If you do not have a privacy framework in place, when do you plan to implement one?

	Responses by Department	
A data privacy framework is already in place.	4	(22%)
6 months to 1 year	5	(28%)
1 to 2 years	8	(44%)
No response	1	(6%)

Q11 Please indicate your level of agreement with each of the following statements:

	Strongly Agree	Agree	Disagree	Strongly Disagree
My EIM roles and responsibilities are adequately funded.	1	7	9	1
My EIM roles and responsibilities are adequately staffed.	0	7	10	1
The EIM Steering Committee adds value for my department.	0	14	4	0
Establishing a shared analytics service center would improve the quality of service by my department.	1	9	8	0
Implementing EIM (EO 2016-24) will benefit my department through improved efficiency.	3	10	5	0
Implementing EIM (EO 2016-24) will benefit my department through better access to data.	3	6	9	0
Implementing EIM (EO 2016-24) will benefit my department through reduced costs.	3	4	8	3
Implementing the EIM program will improve and/or mature our privacy protection processes.	2	13	3	0

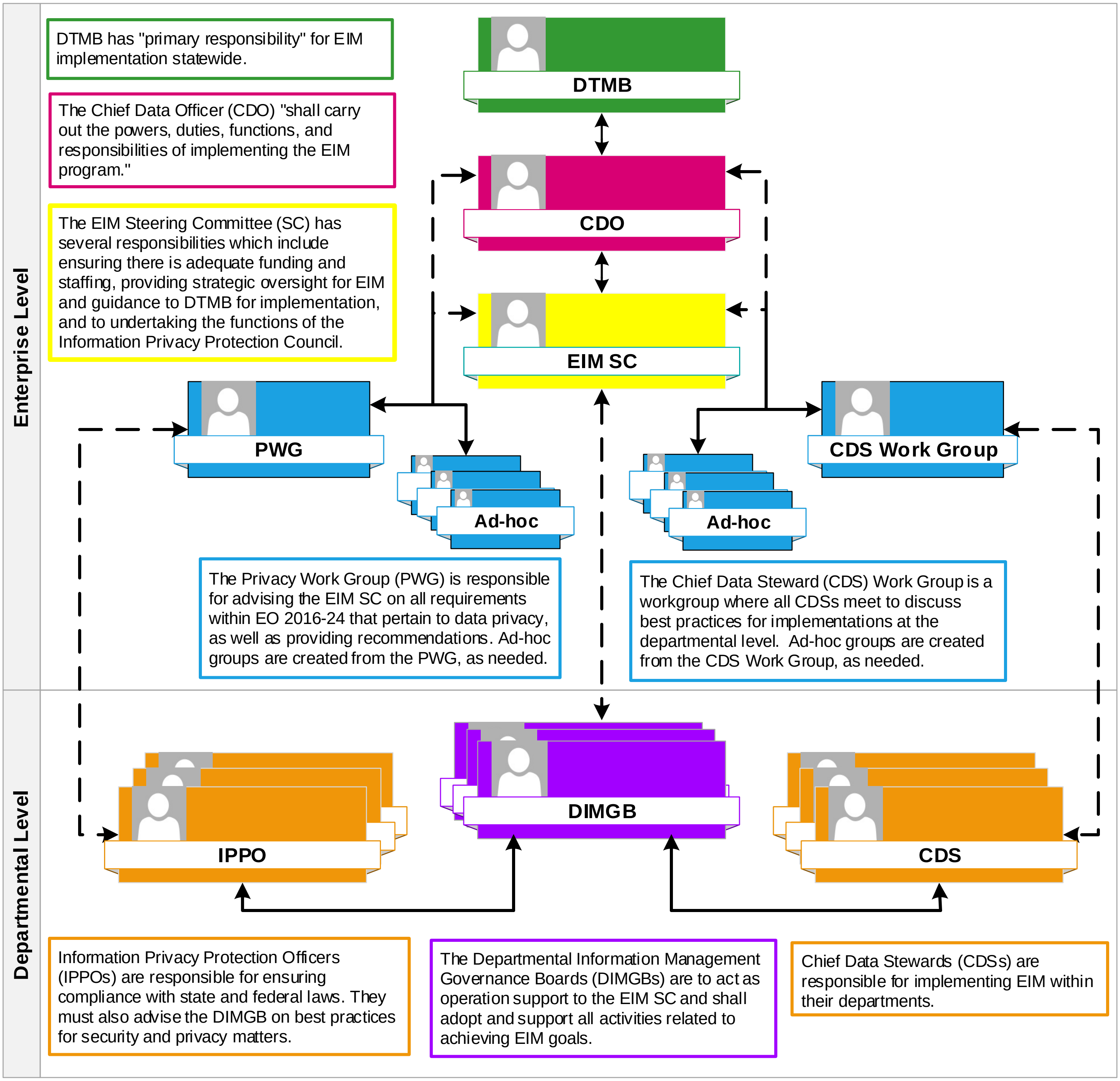
Q12 Does your department have a budget with specific funding that facilitates implementation of EIM?

	Responses by Department	
Yes	16	(89%)
No	2	(11%)

UNAUDITED
Exhibit #4

EXECUTIVE ORDER 2016-24
Department of Technology, Management, and Budget (DTMB)

Responsibility Hierarchy and Flow of Information for Executive Order No. 2016-24



DTMB has "primary responsibility" for EIM implementation statewide.

The Chief Data Officer (CDO) "shall carry out the powers, duties, functions, and responsibilities of implementing the EIM program."

The EIM Steering Committee (SC) has several responsibilities which include ensuring there is adequate funding and staffing, providing strategic oversight for EIM and guidance to DTMB for implementation, and to undertaking the functions of the Information Privacy Protection Council.

The Privacy Work Group (PWG) is responsible for advising the EIM SC on all requirements within EO 2016-24 that pertain to data privacy, as well as providing recommendations. Ad-hoc groups are created from the PWG, as needed.

The Chief Data Steward (CDS) Work Group is a workgroup where all CDSs meet to discuss best practices for implementations at the departmental level. Ad-hoc groups are created from the CDS Work Group, as needed.

Information Privacy Protection Officers (IPPOs) are responsible for ensuring compliance with state and federal laws. They must also advise the DIMGB on best practices for security and privacy matters.

The Departmental Information Management Governance Boards (DIMGBs) are to act as operation support to the EIM SC and shall adopt and support all activities related to achieving EIM goals.

Chief Data Stewards (CDSs) are responsible for implementing EIM within their departments.

Source: The OAG prepared this exhibit using EO 2016-24 and information obtained from DTMB.

DESCRIPTION

EO 2016-24 created an EIM Steering Committee and gave DTMB primary responsibility for implementation of the EO and the EIM program (Exhibit #1). The EIM Steering Committee is chaired by the CDO, an appointee of the DTMB Director (Exhibit #4). EIM Steering Committee membership is composed of representatives of 12 State departments and agencies who meet monthly to set policy and review reports on the progress of the program. The focus of the EIM program is to share data and leverage information across the enterprise. By providing easier access to data among agencies, the State will be able to make quicker data-driven decisions that will be more effective and impactful. The EIM program is a way of managing vast and valuable State information assets. The EIM program is important because citizens should see and expect one State government, despite the fact that government decisions increasingly require more types of data from multiple and diverse government agencies. Citizens should have one central entry point to State systems to see all types of services and program information in which they are interested.

The privacy of PII within the State and with external parties is a critical element of EO 2016-24. The State is faced with a myriad of laws and regulations that protect and provide privacy for confidential information. The State is charged with assessing privacy risks, monitoring programs to mitigate those risks, and instituting a unified privacy framework across the enterprise.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To assess the effectiveness of DTMB's efforts to comply with EO 2016-24 and to provide a status of the State's compliance with EO 2016-24. 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 December 21, 2016 through September 30, 2018.

METHODOLOGY

We conducted a preliminary survey of EO 2016-24. During our preliminary survey, we:

- Determined the EO's requirements (Exhibit #1).

- Interviewed DTMB's EIM program staff and created Exhibit #4, which is a visual presentation of the responsibility hierarchy and flow of information for the execution of EO 2016-24, as developed by the OAG and reviewed and approved by DTMB.

- Attended meetings of the EIM Steering Committee and CDSs to assess their efforts in executing EO 2016-24.

- Attended EIM technology solution walkthroughs.

- Reviewed documentation on the progress toward various elements of the EO based on reports to the EIM Steering Committee and supporting documentation.

OBJECTIVE #1

To assess the effectiveness of DTMB's efforts to comply with EO 2016-24.

To accomplish this objective, we:

- Interviewed DTMB program staff and management.

- Reviewed the PwC contract for Statewide EIM program implementation.

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

- Judgmentally sampled 32 of 62 contact deliverables to assess whether the deliverables were completed as outlined in the contract.

- Reviewed documentation on the progress toward various elements of the EO, including single Internet sign-on, data metrics, business glossary, identity master, location master, DSA repository, DIMGBs, and privacy and security assessments.

- Judgmentally sampled 3 of 16 State departments that had established a DIMGB and reviewed the departments' representatives.

- Reviewed position descriptions of the State's CDSs and IPPOs to assess compliance with DTMB guidance and best practices.

We made our selections using a risk-based approach. Because our selections were judgmental, we could not project our results to the populations.

OBJECTIVE #2

To provide a status of the State's compliance with EO 2016-24.

To accomplish this objective, we:

- Interviewed DTMB staff.

- Assessed and provided the status of selected sections of EO 2016-24 (Exhibit #2).

- Conducted a survey of CDSs and IPPOs (Exhibit #3).

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material conditions* or 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 3 findings and 3 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all of the 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 fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and

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

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 to 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.

SUPPLEMENTAL INFORMATION

Our audit report includes supplemental information presented as Exhibits #1 through #4. Our audit was not directed toward expressing a conclusion on Exhibits #1 and #4. Exhibits #2 and #3 supported the conclusion to our second objective.

GLOSSARY OF ABBREVIATIONS AND TERMS

ASC Analytics Service Center.

CDO Chief Data Officer.

CDS Chief Data Steward.

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 IT.

Departmental Information Management Governance Board (DIMGB) The primary support structure within a department to ensure that the goals of the EIM program are successfully implemented.

DSA data sharing agreement.

DSO Department Security Officer.

DTMB Department of Technology, Management, and Budget.

ED executive directive.

effectiveness Success in achieving mission and goals.

efficiency Achieving the most outputs and the most outcomes practical with the minimum amount of resources.

EIM Enterprise Information Management.

EIM Steering Committee (SC) An advisory committee created to assist DTMB with the execution of EO 2016-24.

EO executive order.

FOIA Freedom of Information Act.

goal An intended outcome of a program or an entity to accomplish its mission.

IPPO Information Privacy Protection Officer.

IT information technology.

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. Our assessment of materiality is in relation to the respective audit objective.

MCS Michigan Cybersecurity Division.

MDHHS Michigan Department of Health and Human Services.

OAG Office of the Auditor General.

observation A commentary that highlights certain details or events that may be of interest to users of the report. An observation may not include the attributes (condition, effect, criteria, cause, and recommendation) that are presented in an audit finding.

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.

personally identifiable information (PII) This includes information such as full name, date of birth, social security number, home address, fingerprints, etc.

PwC PricewaterhouseCoopers.

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.

SOM

State of Michigan.

State Unified Information Technology Environment (SUITE)

The framework used by DTMB to deliver IT projects to State agencies including systems engineering, project management, procurement, and security. SUITE requires adherence to policies and procedures and creation of sound documentation.

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Independent Objective Transparent

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud
Hotline: (517) 334-8060, Ext. 1650