# Office of the Auditor General
Follow-Up Report on Prior Audit Recommendations

# Michigan Cyber Civilian Corps
Department of Technology, Management, and Budget

September 2023

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

071-0519-19F

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.

The auditor general may make investigations pertinent to the conduct of audits.

*Article IV, Section 53 of the Michigan Constitution*

OAG
Office of the Auditor General

# Report Summary

## *Follow-Up Report*

## *Michigan Cyber Civilian Corps (MiC3)*

## *Department of Technology, Management, and Budget (DTMB)*

**Report Number:**
**071-0519-19F**

**Released:**
**September 2023**

We conducted this follow-up to determine whether DTMB had taken appropriate corrective measures in response to one material condition and one reportable condition noted in our September 2019 audit report.

| Prior Audit Information | Follow-Up Results | | |
|---|---|---|---|
| | **Conclusion** | **Finding** | **Agency Preliminary Response** |
| Finding 1 - Material condition<br><br>Further adherence to volunteer requirements needed.<br><br>Agency agreed. | Substantially complied | Not applicable. | |
| Finding 2 - Reportable condition<br><br>Improvements needed to training program.<br><br>Agency agreed. | Substantially complied | Not applicable. | |


**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

This Page Left Intentionally Blank

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

September 12, 2023

Michelle Lange, Director
Department of Technology, Management, and Budget
and
Laura Clark, Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

Director Lange and Chief Information Officer Clark:

This is our follow-up report on the one material condition (Finding 1), one reportable condition (Finding 2), and two corresponding recommendations reported in the performance audit of the Michigan Cyber Civilian Corps, Department of Technology, Management, and Budget. That audit report was issued and distributed in September 2019. Additional copies are available on request or at audgen.michigan.gov.

We appreciate the courtesy and cooperation extended to us during our follow-up. If you have any questions, please call me or Laura J. Hirst, CPA, Deputy Auditor General.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

## TABLE OF CONTENTS

## MICHIGAN CYBER CIVILIAN CORPS

# INTRODUCTION, PURPOSE OF FOLLOW-UP, AND PROGRAM DESCRIPTION

**INTRODUCTION**

This report contains the results of our follow-up of the material condition* (Finding 1), the reportable condition* (Finding 2), and the two corresponding recommendations reported in our performance audit* of the Michigan Cyber Civilian Corps (MiC3), Department of Technology, Management, and Budget (DTMB), issued in September 2019.

**PURPOSE OF FOLLOW-UP**

To determine whether DTMB had taken appropriate corrective measures to address our corresponding recommendations.

**PROGRAM DESCRIPTION**

MiC3 is a program established by Public Act 132 of 2017, as amended, under which civilians may volunteer, at the acceptance of DTMB, to provide rapid response assistance to a municipal, educational, or nonprofit organization during a cybersecurity incident*. The vision of MiC3 is to have an experienced, certified group of subject matter experts across a wide range of cyber defense skills, with knowledge of the tools, techniques, and methods used by attackers against networks and systems, and the expertise to defend those systems.

MiC3 was created in 2013 and was administered by the Merit Network until 2016. Since 2016, MiC3 has been administered by DTMB Cybersecurity and Infrastructure Protection. MiC3 operates under an advisory board composed of the adjutant general and the directors of DTMB, the Michigan Department of State Police (MSP), and the Department of Labor and Economic Opportunity and their designees.

Public Act 132 of 2017 was amended in 2020 to update membership and the scope of response for MiC3. Membership definition was revised to distinguish between deployable members and nondeployable advisors and define their responsibilities.

As of June 2, 2023, there were 69 MiC3 deployable members and 1 nondeployable advisor consisting of individuals from the government, academia, business, financial, and healthcare sectors. Since program inception, DTMB has deployed MiC3 volunteers to 2 cyber-incidents at local governments. Each deployment involved volunteers being sent on site to assist in assessing the incident and providing remediation recommendations to the client.

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

From October 1, 2021 through June 30, 2023, DTMB had expended $299,204 on the program:

MiC3 Expenditures

| Category | Total | Percentage |
|---|---|---|
| Training and continuing education | $156,320 | 52% |
| Program manager | 131,252 | 44% |
| Miscellaneous expenses | 6,593 | 2% |
| Program coordinator | 5,040 | 2% |
| Total | $299,204 | 100% |

## PRIOR AUDIT FINDINGS AND RECOMMENDATIONS, AGENCY PLAN TO COMPLY, AND FOLLOW-UP CONCLUSIONS

### FINDING 1

Audit Finding Classification: Material condition.

Summary of the September 2019 Finding:
DTMB did not ensure all MiC3 volunteers met program requirements, leaving many volunteers ineligible to fully participate in the program and deploy to cyber-incidents. Specifically, we noted DTMB did not:

a. Adequately contract with volunteers to ensure acceptance of the terms and conditions of membership in the program.

b. Ensure all volunteers underwent sufficient background checks.

c. Sufficiently evaluate the qualifications of all volunteers.

d. Ensure all volunteers had support from their employer to participate in the program.

Recommendation Reported in September 2019:
We recommended DTMB ensure all MiC3 volunteers meet program requirements to ensure eligibility to participate in the program and deploy to cyber-incidents.

**AGENCY PLAN TO COMPLY***

On April 24, 2020, DTMB indicated:

- As of May 14, 2019, the Attorney General provided DTMB with an updated volunteer agreement compliant with Public Act 132 of 2017, as amended.

- As of September 3, 2019, DTMB has communicated documentation and background check requirements to volunteers and is currently in the process of reviewing member's submitted information to ensure compliance with DTMB policy and Public Act 132 of 2017, as amended.

- As of October 1, 2019, DTMB has started the web application enhancement project to replace manual processes. Specifically, the improvements include enabling uploads of resumes and other required documentation by applicants and current volunteers.

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

**FOLLOW-UP CONCLUSION**

Substantially complied.

Our review of the program requirements for the 70 active MiC3 volunteers as of June 2, 2023 noted DTMB:

a. Complied.

   DTMB adequately contracted with all 70 volunteers; 69 (99%) of 70 contracts were signed by DTMB and contained the volunteers' attestation to their standard of expertise.

b. Complied.

   DTMB ensured all volunteers underwent sufficient background checks. We noted MSP and the Federal Bureau of Investigation (FBI) criminal background checks were completed for all 70 volunteers. Also, background checks were passed by all of the deployable volunteers.

c. Complied.

   DTMB sufficiently evaluated the qualification of volunteers. Resumes for all 70 volunteers demonstrated they met the required level of experience.

   Also, DTMB provided records to demonstrate required tests had been passed for 57 (81%) of 70 volunteers.

   DTMB did not have complete testing records for the remaining 13 (19%) of 70 volunteers. However, DTMB provided communications with the individuals to demonstrate they were onboarded into the program by Merit, the company who previously administered MiC3.

d. Partially complied.

   DTMB did not always ensure all volunteers had support from their employer to participate in the program. We noted letters of support existed for all 70 volunteers; however, 9 (13%) of 70 letters were unsigned by the employer.

## FINDING 2

Audit Finding Classification: Reportable condition.

Summary of the September 2019 Finding:
DTMB should improve its training program to ensure MiC3 volunteers receive beneficial and cost-effective training. Our review of the training program disclosed DTMB:

a. Did not hold volunteers accountable for attending training or receiving corresponding certifications from the training administered. Specifically, DTMB did not:

   (1) Ensure volunteers obtained certifications upon completion of the training.

   (2) Ensure all volunteers attended training.

b. Did not formally evaluate the effectiveness of the training provided.

c. Should consider using a greater variety of training vendors.

Recommendation Reported in September 2019:
We recommended DTMB improve its training program to ensure MiC3 volunteers receive beneficial and cost-effective training.

**AGENCY PLAN TO COMPLY**

On April 24, 2020, DTMB indicated it would write a formal training policy to determine training needs, procure vendors, evaluate the training provider, and keep thorough records. Also, DTMB would revise the charter to establish annual program goals, update the roles and responsibilities to include new training documentation requirements, and write a formal cyber-incident deployment policy.

**FOLLOW-UP CONCLUSION**

Substantially complied.

Our follow-up noted DTMB:

a. Partially complied.

   Section 18.230(4) of the *Michigan Compiled Laws* states DTMB may provide appropriate training to volunteers. Starting in 2021, DTMB annually prepays for 60 accounts with a third-party vendor to provide online on-demand training. We noted 39 (65%) of 60 accounts were utilized by volunteers between October 2021 and June 2, 2023. We verified a portion of volunteers are completing the training; however, DTMB did not ensure all volunteers utilized it or consider reducing the number of prepaid accounts.

b. Partially complied.

   DTMB performed monthly meeting calls with volunteers and discussed available training to encourage training participation; however, detailed discussions and feedback were not maintained. Also, DTMB did not regularly obtain volunteer feedback data available from the online training vendor to evaluate the effectiveness and usefulness of the training.

c. Complied.

   DTMB previously contracted with a third-party vendor to provide annual cybersecurity training and corresponding certifications to volunteers. Starting in 2021, DTMB contracted with a different third-party vendor to provide online on-demand training to volunteers. DTMB is still utilizing one training vendor; however, the new format provides 243 unique cybersecurity courses available anytime at a cost reduction of 55% from the prior vendor. Also, advisory board meetings were held to discuss future opportunities to use additional vendors.

## FOLLOW-UP METHODOLOGY AND PERIOD

**METHODOLOGY**

We reviewed DTMB's corrective action plan and updated legislation impacting the program. Specifically, for:

- Finding 1, we:
    - Met with DTMB staff to obtain an understanding of DTMB's processes to ensure volunteers met program requirements.
    - Reviewed documentation for all 69 deployable members and 1 nondeployable advisor to determine whether DTMB ensured volunteers:
        - Passed the required onboarding tests.
        - Signed a contract with DTMB, including an attestation to their standard of expertise.
        - Passed the required background checks.
        - Obtained a signed agreement from their employer to participate in the program.
        - Met the required level of experience.
- Finding 2, we:
    - Reviewed the third-party training vendor data to identify how many volunteers were utilizing the training provided and paid for by DTMB.
    - Evaluated DTMB communications with members to determine if the training being provided was being evaluated for its effectiveness.
    - Met with DTMB staff to obtain an understanding of the variety of training topics provided to members.

**PERIOD**

Our follow-up generally covered October 1, 2021 through June 30, 2023.

## GLOSSARY OF ABBREVIATIONS AND TERMS

| | |
|---|---|
| **agency plan to comply** | The response required by Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100). The audited agency is required to develop a plan to comply with Office of the Auditor General audit recommendations and to submit the plan to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, 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. |
| **cybersecurity incident** | An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information residing on any of these. A cybersecurity incident includes, but is not limited to, the existence of a vulnerability in an information system, system security procedures, internal control, or implementation that is subject to exploitation. Cybersecurity incident was shortened to "cyber-incident" in this report. |
| **DTMB** | Department of Technology, Management, and Budget. |
| **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. |
| **MiC3** | Michigan Cyber Civilian Corps. |
| **MSP** | Michigan Department of State Police. |
| **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. |

| | |
|---|---|
| **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: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud. |

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


**Report Fraud/Waste/Abuse**

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070