Office of the Auditor General
Performance Audit Report

Michigan Cyber Civilian Corps

Department of Technology, Management, and Budget

September 2019

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

071-0519-19

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

Performance Audit

Michigan Cyber Civilian Corps (MiC3)

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0519-19

Released:
September 2019

MiC3 is a program established by Public Act 132 of 2017 under which civilians may volunteer, at the invitation of DTMB, to provide rapid response assistance to a municipal, educational, nonprofit, or business organization during a cyber-incident. MiC3 is administered by DTMB Cybersecurity and Infrastructure Protection, which has deployed MiC3 volunteers in response to two cyber-incidents at local governments. As of February 2019, there were 99 MiC3 volunteers, consisting of individuals from the government, academia, business, financial, and healthcare sectors. Over the life of the program, MiC3 expenditures totaled $1.5 million as of April 2019.

Audit Objective			**Conclusion**
Objective: To assess the effectiveness of DTMB's administration of MiC3.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Not all MiC3 volunteers met program requirements, leaving many volunteers ineligible to fully participate in the program and deploy to cyber-incidents. Background checks were not completed for 35% of volunteers, and 2% of volunteers failed the background check (Finding #1).	X		Agrees
Volunteers were not held accountable for attending training or receiving corresponding certifications from the training administered. DTMB paid $28,789 in examination costs for volunteers who did not receive certifications (Finding #2).		X	Agrees
Observations Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
MiC3 is in an initial state of maturity. Volunteers do not have access to an approved set of tools to use when responding to cyber-incidents (Observation #1).	Not applicable for observations.		

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

September 13, 2019

Ms. Tricia L. Foster, Director
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Ms. Foster:

This is our performance audit report on the Michigan Cyber Civilian Corps, Department of Technology, Management, and Budget.

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 to the State Budget Director 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.

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

MICHIGAN CYBER CIVILIAN CORPS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

ADMINISTRATION OF THE MICHIGAN CYBER CIVILIAN CORPS

BACKGROUND

The Michigan Cyber Civilian Corps (MiC3) is a program under which civilian volunteers, who possess cybersecurity incident* response expertise, provide assistance to organizations during cyber-incidents. MiC3 is administered by Department of Technology, Management, and Budget (DTMB) Cybersecurity and Infrastructure Protection.

AUDIT OBJECTIVE

To assess the effectiveness* of DTMB's administration of MiC3.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Survey responses of 38 MiC3 volunteers generally indicated satisfaction with the training program.
- Recommendations were successfully provided to both local governments that accepted MiC3 assistance through a deployment.
- MiC3 is the first of its kind in the United States, winning the 2017 National Association of State Chief Information Officers (NASCIO) award in business continuity and disaster recovery as well as the 2017 StateScoop 50 award in IT innovation.
- One material condition* related to volunteers not meeting program requirements (Finding #1).
- One reportable condition* related to improving the training program (Finding #2).

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

FINDING #1

Further adherence to volunteer requirements needed.

DTMB did not ensure that all MiC3 volunteers met program requirements, leaving many volunteers ineligible to fully participate in the program and deploy to cyber-incidents.

Public Act 132 of 2017 establishes various requirements for MiC3 volunteers. Specifically, Section 18.230(2)(a) of the *Michigan Compiled Laws* requires that DTMB publish guidelines that include an explanation of the standard used to determine whether an individual may serve as an MiC3 volunteer.

Our review of the program requirements for the 99 active MiC3 volunteers as of February 2019 disclosed that DTMB did not:

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

   Section 18.224 of the *Michigan Compiled Laws* requires that DTMB enter into a contract with any individual who wishes to accept an invitation to serve as an MiC3 volunteer. The volunteer contract contains requirements such as nondisclosure of confidential information, compliance with State security policies and procedures, and disclosure of conflicts of interest.

   We noted:

   (1) Contracts did not exist for 25 (25%) of the 99 volunteers.

   (2) DTMB did not sign any of the existing 74 contracts.

   (3) The volunteer name was not listed within 42 (57%) of the 74 contracts.

   (4) Volunteers did not attest to their standard of expertise within any of the 74 contracts as required by Section 18.224(f) of the *Michigan Compiled Laws*.

b. Ensure that all volunteers underwent sufficient background checks.

   Section 18.225 of the *Michigan Compiled Laws* requires that, when an individual accepts an invitation to serve as an MiC3 volunteer, DTMB shall request the Michigan Department of State Police (MSP) to conduct a criminal background check and criminal records check through the Federal Bureau of Investigation (FBI) on the individual. Based on the background check results, MSP indicates whether the individual is cleared or not cleared to become an MiC3 volunteer. We noted:

   Background checks were not completed for 35% of volunteers, and 2% of volunteers failed the criminal background check.

   (1) Neither the MSP criminal background check nor the FBI criminal records check were completed for 35 (35%) of the 99 volunteers.

   (2) Two (2%) of the 99 volunteers failed the criminal background check.

(3) The FBI criminal records check was not completed for 22 (22%) of the 99 volunteers.

c. Sufficiently evaluate the qualifications of all volunteers.

DTMB requires that all volunteers have at least two years of direct involvement with information security and possess a basic security certification. Also, volunteers are required to pass a series of tests to demonstrate basic networking and security knowledge, including incident response and forensic skills. We noted:

(1) Fourteen (14%) of the 99 volunteers did not pass all components of the required tests.

(2) DTMB did not ensure that 23 (23%) of the 99 volunteers met the required level of experience.

(3) Records were not provided by DTMB to support that the required tests had been passed for 11 (11%) of the 99 volunteers.

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

DTMB requires that all volunteers provide a letter of support from their employer to ensure availability to participate in MiC3 program activities. We noted:

(1) Letters of support did not exist for 33 (33%) of the 99 volunteers.

(2) Employers did not sign 4 (6%) of 66 letters of support that did exist.

DTMB deployed MiC3 volunteers to two cyber-incidents since program inception in 2013. For these two deployments, participating volunteers either attended a scoping call where sensitive details of the cyber-incident were discussed or were physically deployed to assist the client on site.

The following table summarizes the requirement status of each volunteer involved in the two deployments:

		Role			Experience		Volunteer Contract			Volunteer Name	Employer
Volunteer	Deployment	Deployed	Scoping Call	Required Tests Not Passed	Requirement Not Validated	Background Check Status	Did Not Exist	Not Signed by DTMB	Did Not Contain Volunteer Attestation of Standard of Expertise	Not Listed Within Volunteer Contract	Letter of Support Did Not Exist
1	1		Yes	X		Partially Completed		X	X		
2	1	Yes	Yes			Clear		X	X		
3	1		Yes		X	Clear	X	N/A	N/A	N/A	X
4	1		Yes			Denied		X	X		
5	1	Yes	Yes			Clear		X	X	X	
6	1		Yes			Not Completed		X	X	X	X
7	1 and 2	Yes	Yes		X	Clear		X	X		
8	2	Yes	Yes			Clear		X	X		
9	2	Yes	Yes			Clear		X	X		
10	2	Yes	Yes			Clear		X	X		
11	2	Yes	Yes			Clear		X	X	X	
12	2		Yes			Clear		X	X	X	
13	2		Yes			Clear		X	X		
14	2	Yes				Clear		X	X		
15	2	Yes	Yes			Clear		X	X	X	
16	2		Yes			Clear		X	X		
17	2	Yes				Clear		X	X	X	

N/A - Not applicable because Volunteer 3 was the program manager and did not have a volunteer contract.

DTMB informed us that it has placed emphasis on increasing the number of volunteers while requirements of membership in the program have evolved.

We consider this finding to be a material condition as it directly hinders MiC3 from achieving its objective of responding to cyber-incidents using qualified volunteers as defined within the *Michigan Compiled Laws* and other program requirements.

RECOMMENDATION

We recommend that DTMB ensure that all MiC3 volunteers meet program requirements to ensure eligibility to participate in the program and deploy to cyber-incidents.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the finding as indicated below:

a. *Going forward, DTMB will require all members to sign a volunteer agreement. A revised volunteer agreement that includes an attestation clause has been reviewed and approved by the Department of Attorney General. DTMB is now using this revised agreement to on-board all new MiC3 members and has commenced a process to have all current members re-sign the new agreement.*

   DTMB agrees that the records management process for the MiC3 program needs improvement. The first half of the application and onboarding process was automated beginning in 2017 and plans are in place to automate the remaining steps of the application and onboarding process in fiscal year 2020. The manual portion of the onboarding process has been improved throughout fiscal years 2018 and 2019 to help reduce the margin of error and improve response time. DTMB

continues to review and improve its records management procedures for the MiC3 program. Furthermore, DTMB's Chief Security Officer has signed all the volunteer agreements of MiC3 volunteers who have met all requirements to fully participate in the program.

b. *Going forward, background screening will be required of all members who wish to gain access to State secured facilities and/or respond to a cybersecurity incident when a client has requested assistance. Applicants who have passed the assessment testing but have not completed all the steps of the Michigan State Police (MSP) criminal background check and/or the Federal Bureau of Investigation (FBI) criminal records check have been allowed to participate in the monthly networking calls, yearly training opportunities, and/or other networking opportunities offered by the program as part of the recruitment initiative efforts. One member who failed the criminal background check was already a member of the program under the Merit Network, prior to PA132. This individual is one of the original members of the program. In March of 2018, this member received the denied status on the background check that became a requirement effective January 2018. DTMB explained to this member that he/she would have limited access to the program benefits going forward. The member was allowed to benefit from the networking opportunities and yearly training; however, it was made abundantly clear that he/she would not be eligible to deploy or gain access to any client or State building and/or privileged or sensitive information. DTMB learned of the second member who received a denied background check status on March 1, 2019.*

   As of April 2019, both members have had their status as MiC3 volunteers revoked.

c. *The first step in the application process is a series of assessment tests in which an applicant must pass four out of the five tests in order to officially begin the onboarding process. The program was previously managed under the Merit Network which used these same 5 assessment tests and as such, the acquired members were not retested when it migrated to DTMB management beginning fiscal year 2017. Although DTMB retained overall program responsibility, DTMB was not able to provide testing records previously administered by the Merit Network. DTMB agrees that the manual records management process needs improvement and has already begun efforts to ensure that proper and current documentation is on file for each member.*

d. *Although PA132 does not require that DTMB enforce this request and it was not viewed as a disqualifier of membership for various reasons, DTMB will now make this part of the required documentation for membership and policies and procedures will be reviewed to determine if there is a need to create an exceptions process for the employer agreement.*

FINDING #2

DTMB should improve its training program to ensure that MiC3 volunteers receive beneficial and cost-effective training.

Improvements needed to training program.

National Institute of Standards and Technology* (NIST) Special Publication 800-50 states that a training program is crucial to ensuring that individuals have the information needed in order to do their jobs. Also, NIST states that formal evaluation and feedback mechanisms are critical components of any training program to ensure that objectives are being met and that continuous improvement of the program occurs.

DTMB contracted with a third party vendor from 2016 through 2018 to provide annual cybersecurity training and corresponding certifications to MiC3 volunteers. Our review of the training program disclosed that DTMB:

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

   (1) Ensure that volunteers obtained certifications upon completion of training. Our analysis of training records and online certification records disclosed:

	Fiscal Year		
Number of Volunteers Who	2016	2017	2018
Received certification	21 (68%)	28 (74%)	47 (69%)
Did not receive certification	10 (32%)	10 (26%)	21 (31%)
Total	31 (100%)	38 (100%)	68 (100%)

DTMB pays the vendor an established fee so that volunteers may take the examinations necessary to obtain the training certifications. DTMB paid $28,789 in examination costs over the three years for volunteers who did not receive these certifications.

Volunteers may not obtain certifications for various reasons, including not taking or passing the required examinations. DTMB should establish a formal process to confirm that volunteers obtained these certifications and follow up with those who did not.

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

(2) Ensure that all volunteers attended training. We analyzed volunteer sign-in sheets for each training session and noted:

	Fiscal Year		
Volunteers Attended	2016	2017	2018
All days	n/a	11 (29%)	44 (65%)
1 - 4 days	n/a	24 (63%)	19 (28%)
0 days	n/a	3 (8%)	5 (7%)
Total volunteers	31 (100%)	38 (100%)	68 (100%)

n/a - Not available because DTMB was unable to provide us with daily sign-in sheets for fiscal year 2016.

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

According to NIST, evaluating effectiveness is a vital step to ensure that training is cost-effective and satisfies the organization's needs. Evaluating the effectiveness of training could include activities such as:

- Identifying how useful the participants found the training.
- Determining whether participants improved their knowledge and skills.
- Assessing the measurable program benefits achieved as a result of the training.

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

NIST states that prior to selecting a particular training vendor, organizations should obtain a thorough understanding of their training needs and determine if the prospective vendor's material meets those needs.

According to Department of Defense Directive (DoDD) 8570, a number of vendors offer training certifications for specific information assurance functions, such as incident response and forensics. Diversifying its training vendors would allow DTMB to further develop the knowledge and skills of volunteers in accordance with their individual training needs.

DTMB informed us that it has used this specific training program as an incentive to join MiC3 based on feedback from volunteers. DTMB also informed us that it had not developed a method for holding MiC3 volunteers accountable when training was not attended or certifications were not obtained.

RECOMMENDATION

We recommend that DTMB improve its training program to ensure that MiC3 volunteers receive beneficial and cost-effective training.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the finding as indicated below:

a. *In fiscal year 2016, although DTMB retained overall program responsibility, the program was managed under the Merit Network and DTMB was not able to provide evidence of sign-in sheets. DTMB requires members to commit to the annual training in advance. DTMB agrees that the methods used to track attendance were not as thorough as they could have been; however, the importance of attendance was stressed to those who committed. Some members were unable to pass the exam on their first try which is common in the cybersecurity field for high skill certifications.*

b. *Although DTMB agrees that it did not adequately evaluate the effectiveness of the training provided, the usefulness and value of the selected training were discussed frequently with volunteers in MiC3 monthly teleconferences and feedback for improvement was sought. DTMB will follow best practices for formally assessing the training benefits achieved and usefulness to participants going forward.*

c. *DTMB will ensure that its formal training vendor selection methodology is documented, and that training is based on the needs of the program and its volunteer members' individual training needs. DTMB will document the program needs assessment and justification for vendor selection going forward.*

OBSERVATION #1

Program in initial state of maturity.

MiC3 is in an initial state of maturity. While the program began operations in 2013, the Cyber Civilian Corps Act (Public Act 132 of 2017), which formally defined program requirements and allowed for deployment of volunteers (without a Governor declared state of emergency), was not made effective until 2018.

DTMB should consider completing the following actions to further mature MiC3:

MiC3 volunteers do not have access to an approved set of tools that can be used to assist clients in responding to cyber-incidents.

- Define a set of tools to assist in incident response and forensics during deployments as required by Section 18.230(1)(a) of the *Michigan Compiled Laws*. MiC3 volunteers did not have access to approved tools that could be used to assist clients in responding to cyber-incidents.

- Continue to increase the exposure of MiC3 to the public in order to meet the program's goals of resolving cybersecurity threats and increasing awareness. As of April 2019, and although the program began operations in 2013, DTMB had deployed MiC3 volunteers two times.

- Conduct additional training exercises with involvement from all active volunteers to ensure readiness for deployments. Survey responses from 29 volunteers regarding recommendations for improving MiC3 disclosed that 9 (31%) felt that additional exercises were needed.

- Create detailed policies and procedures to be followed when responding to cyber-incidents on deployments. Policies and procedures will help provide guidance to volunteers on decision-making and specific actions to be taken and will also define the boundaries the volunteers are operating within.

- Seek legislative changes to further define the requirements of individuals who wish to participate in the MiC3 training program. Section 18.230(4) of the *Michigan Compiled Laws* allows DTMB to provide appropriate training to individuals who wish to participate in MiC3 and to existing MiC3 volunteers. As currently worded, the law allows any interested individuals to obtain training at no cost to them even if they do not or cannot meet specified requirements of the program.

- Increase advisory board participation in the program, including review of all policies and procedures as required by Section 18.229(3) of the *Michigan Compiled Laws*.

- Finalize the contract with clients that defines the requirements for obtaining assistance through MiC3. This should include formally defining the criteria to be met in order for MiC3 to deploy resources to the client. As of February 2019, the contract was in draft form.

- Update the wording of the employer letter of support to ensure full availability of volunteers and understanding of program commitments by employers. The letter states that MiC3 volunteers may only be deployed during a Governor-declared state of emergency; however, Public Act 132 of 2017 allows volunteers to be deployed to any cyber-incident upon approval of the DTMB director.

- Develop a method to assess the potential severity of cyber-incidents, such as by level of impact and urgency, in order to prioritize deployments.

Completion of these actions may improve the effectiveness and public awareness of MiC3 program operations and increase the program to a higher state of maturity.

PROGRAM DESCRIPTION

MiC3 is a program established by Public Act 132 of 2017 under which civilians may volunteer, at the invitation of DTMB, to provide rapid response assistance to a municipal, educational, nonprofit, or business organization during a cyber-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, MSP, and the Department of Talent and Economic Development (TED), or their designees.

The strategic goals of MiC3 are as follows:

- Collaborating to resolve common cybersecurity and infrastructure protection threats to government and private businesses in the State of Michigan.
- Assisting clients who experience cyber-incidents and require assistance because of a lack of internal resources.
- Expanding the cybersecurity awareness and culture throughout the State of Michigan.
- Building relationships among fellow cybersecurity experts to keep lines of communication open in the event of a cybersecurity emergency event.
- Sharing knowledge and experience on new and emerging technologies that combat cybersecurity and infrastructure protection threats.

As of February 2019, there were 99 MiC3 volunteers, consisting of individuals from the government, academia, business, financial, and healthcare sectors. Since program inception, DTMB has deployed MiC3 volunteers to two 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. Also, as a benefit of membership and to increase volunteer skillsets, DTMB offers training and security certifications to MiC3 volunteers through a third party vendor.

As of April 2019, DTMB had expended $1.5 million on MiC3 as follows:

MiC3 Expenditures

Category	Total	Percentage
Training and certifications	$ 666,992	45%
Merit Network - Recruiting and administration	450,000	30%
Program manager - Consultant	204,527	14%
Program coordinator - Consultant	156,540	11%
Miscellaneous expenses	2,729	0%
Total	$1,480,787	100%

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the activities and records of MiC3. 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 July 1, 2016 through April 30, 2019.

METHODOLOGY

We conducted a preliminary survey of MiC3 in order to establish our audit objective, scope, and methodology. During our preliminary survey, we:

- Interviewed MiC3 management and staff regarding their functions and responsibilities.
- Reviewed MiC3 policies and procedures and laws and regulations applicable to the program.
- Analyzed program expenditures for fiscal years 2016 through 2018.
- Obtained an understanding of the volunteer application process and training program.
- Researched similar cybersecurity programs within other governmental entities.

OBJECTIVE

To assess the effectiveness of DTMB's administration of MiC3.

To accomplish this objective, we:

- Tested the eligibility requirements of all 99 active MiC3 volunteers as of February 2019.
- Reviewed training attendance and certification records and assessed the associated expenditures.
- Surveyed the 99 active MiC3 volunteers and evaluated the 38 responses received to determine volunteer

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

involvement, assess program readiness, and seek feedback regarding the effectiveness of program activities.

- Reviewed program exercises, meeting notes, and the results of the two deployments of MiC3 volunteers to cyber-incidents.

- Compared the requirements of the Cyber Civilian Corps Act (Public Act 132 of 2017) against existing policies, procedures, and business processes.

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 2 findings and 2 corresponding recommendations. DTMB's preliminary response indicates that it agrees with both 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 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 to the State Budget Director 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.

GLOSSARY OF ABBREVIATIONS AND TERMS

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.
effectiveness	Success in achieving mission and goals.
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.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
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.

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.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8060, Ext. 1650