Michigan Cyber Civilian Corps (MiC3)

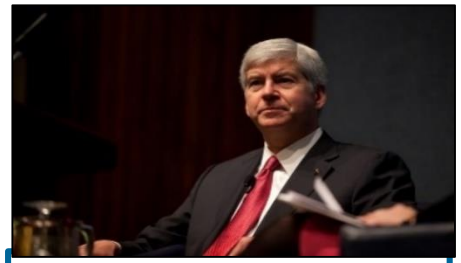
House Oversight Committee

Chris DeRusha
Chief Security Officer

10 October 2019

DTMB

MiC3 History: How We Got Here



Governor Rick Snyder announces MiC3 at 2013 North American International Cyber Summit

2013

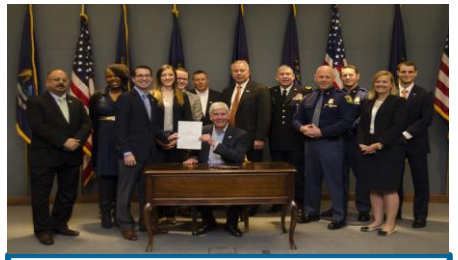
Partnership between the State of Michigan and the Merit Network

2015

Decision made to consolidate program management within State of Michigan

2016

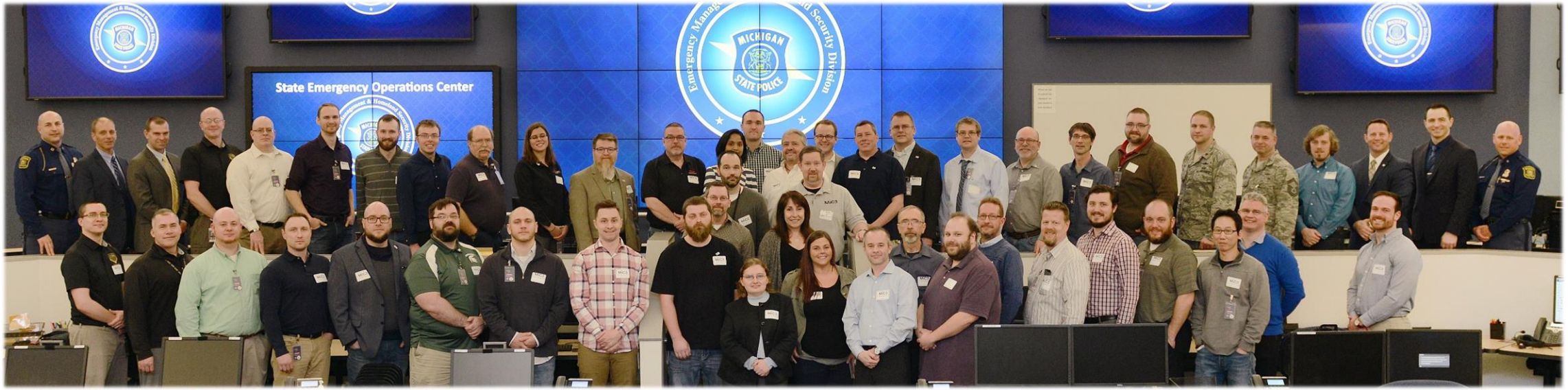
21st Century Infrastructure Commission Report (Communications) Gov. Snyder sets goal of expanding MiC3 to 100



Public Act 132 of 2017 was signed into law by Governor Snyder which provided a framework for operations

2017

MiC3 Helps Victims



- Reserve corps of cyber incident response professionals from across the State, available to respond to and mitigate cyber incidents.
- Public Act 132 passed in 2017 – enhancing authorities and providing liability protections.
- Over 100 MiC3 volunteers with 20 new members in the pipeline.
- Three deployments to local government and critical infrastructure to-date in 2019.

Office of Auditor General Performance Audit – Finding #1

Finding #1: (Material): 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.

DTMB Response:

- Revised onboarding documents cleared by the Attorney General's Office to ensure compliance with *Public Act 132 of 2017*.
- Designed and will soon commence implementation of an automated record keeping system, which will reduce data entry error and allow self-service capabilities for volunteers.
- Developed plan to improve reporting capability to assess member location, expertise and professional activities.
- Developed plan to increase governance: Quarterly record keeping meetings and more frequent engagement with the MiC3 Advisory Board.

Office of Auditor General Performance Audit – Finding #2

Finding #2: DTMB should improve its training to ensure that MiC3 volunteers receive beneficial and cost-effective training.

DTMB Response:

- Assessed deployment training needs and designed and implemented a new training curriculum in July 2019.
- Evaluated 2019 training session to determine effectiveness.
- Developing plan to define critical incident response skills and needs to enhance future training efforts.
- Identifying organizations to benchmark our training methodologies against and inform enhancements to our program.

Office of Auditor General Performance Audit Observations

Observation: 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.

DTMB Response:

- MiC3 volunteers are using experience from incidents to identify and recommend specific tools.
  - This year's training (Security Onion) is an example; this toolset will be recommended to the Advisory Board for official approval.
- DTMB supports refining language in Section 18.230(4) of *Michigan Compiled Laws* to increase requirements for potential volunteers to participate in training.

Observation: 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.

DTMB Response:

- MiC3 volunteers have deployed to a total of three incidents in 2019.
  - Background: DTMB was not authorized to deploy volunteers until January 2018.
- MiC3 does participate in public relations events and conferences as frequently as possible, including the North American International Cybersecurity Summit and the GrrCON cybersecurity conference.

Office of Auditor General Performance Audit Observations

Observation: 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.

DTMB Response:

- Training exercises are scheduled to permit the greatest participation from the largest number of members.
- Members also actively seek out and present new material to other members using Slack and other collaboration methods.
- DTMB will develop additional training opportunities as we continue to define response roles and skill gaps.

Office of Auditor General Performance Audit Observations

Observation: 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.

DTMB Response:

- DTMB drafted a deployment Memorandum of Agreement for prospective clients (on request) and cleared it with the Attorney General's Office.
- DTMB will develop a Standard Operating Procedure to guide MiC3 deployments.
- Any proposed changes will be reviewed by the MiC3 Advisory Board and approved by the State CIO or their designee.

Office of Auditor General Performance Audit Observations

Observation: 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.

DTMB Response:

- DTMB supports legislative changes to distinguish between “deployable” and “non-deployable” volunteers.
- DTMB supports legislative changes to better define eligibility requirements for state funded training.

Observation: 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.

DTMB Response:

- DTMB will hold Quarterly record keeping meetings with management to ensure alignment with established policies.
- DTMB will host Quarterly MiC3 Advisory Board meetings to address operational procedures and associated policies.

Observation: 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.

DTMB Response:

- DTMB drafted a deployment Memorandum of Agreement for prospective clients (on request) and cleared it with the Attorney General's Office.
- DTMB supports legislative changes to task DTMB with formally defining criteria for MiC3 to deploy resources.

Observation: 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.

DTMB Actions:

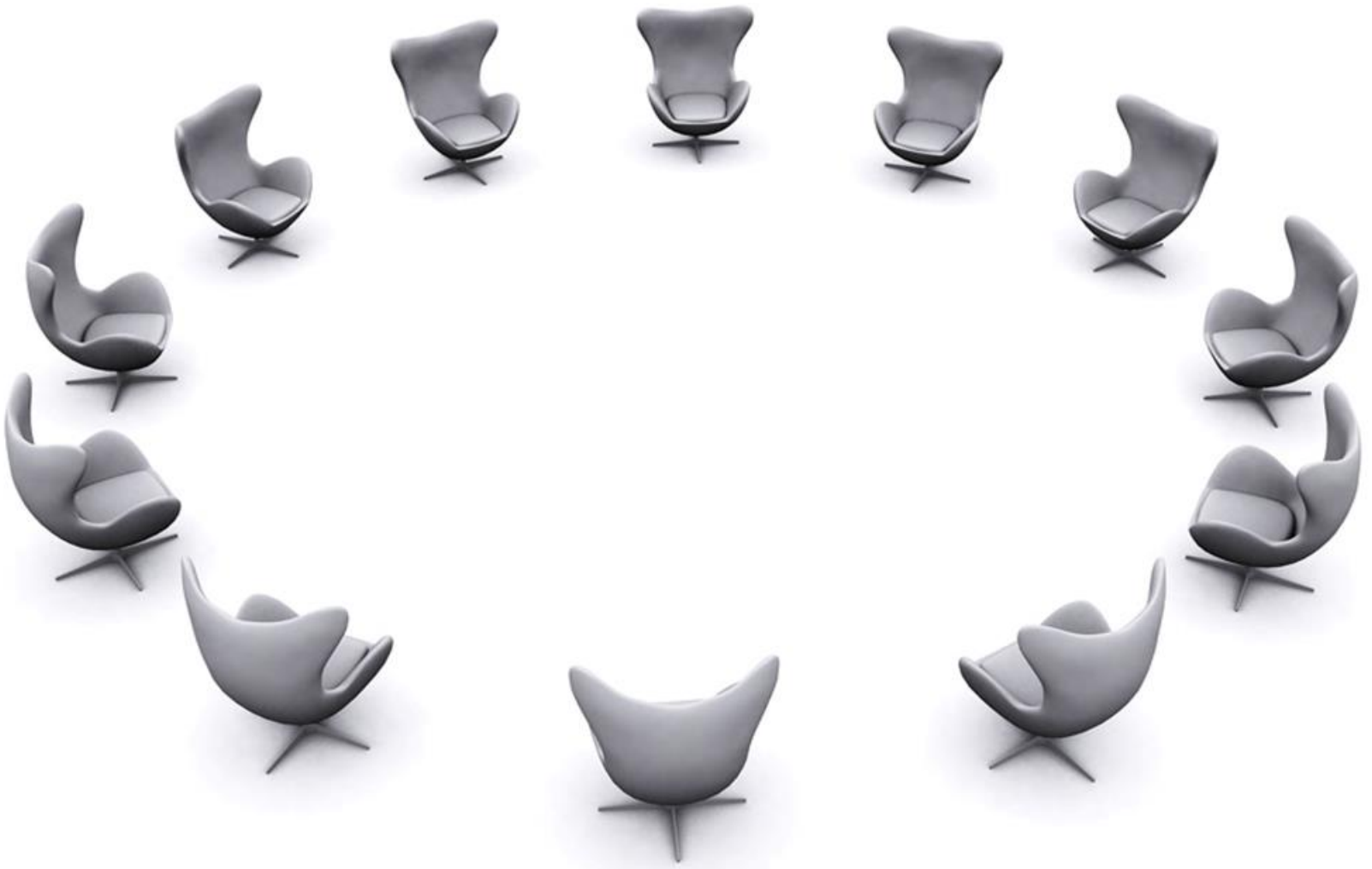
- DTMB has updated the employer letter of support to reflect authorities in *Public Act 132 of 2017* and cleared the updated letter with the Attorney General.

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

DTMB Response:

- DTMB will develop clear thresholds and criteria for prioritizing future MiC3 deployments.

Questions?



Michigan Cyber Contact Information

Chris DeRusha
Chief Security Officer
derushac@michigan.gov

Laura Clark
Deputy Chief Security Officer
ClarkL17@michigan.gov

Derek Larson
Chief of Staff
larsond4@michigan.gov

Chad Laidlaw
Senior Advisor to Chief Security Officer
laidlawc@michigan.gov