BUILDING A CIVILIAN CYBER CORPS

Background

Whenever a natural disaster strikes a community, dozens, if not hundreds, of volunteers flock to assist in any way they can. From re-building homes to cooking food, volunteers work side by side with state and local officials to assist their neighbors. Without these volunteers, state and local governments would struggle to provide adequate services to all those in need. Unfortunately, such volunteer networks do not exist to assist private citizens, small businesses, and public agencies that fall victim to cyber attacks. The state of **Michigan** created the Cyber Civilian Corps to fulfill that need. This volunteer group, consisting of vetted security experts, expands the state's ability to assist public and private entities defend and recover their systems. This document describes the Michigan Cyber Civilian Corps (MiC3) and offers recommendations for other states interested in establishing their own cyber volunteer organization.

History of the Michigan Cyber Civilian Corps

At the 2013 North American International Cyber Summit, Michigan Gov. Rick Snyder announced the launch of an innovative initiative. This initiative would create a corps of volunteer cybersecurity experts who would work side by side with state IT employees to enhance the state's response capacity during a cyber incident.[1] The Michigan Cyber Civilian Corps (MiC3) fulfilled this vision.

The MiC3 began as a partnership among the state's Department of Technology, Management and Budget, the state's volunteer registry system, and the Merit Network (Merit). Volunteer recruitment initially depended on Merit and word of mouth. Interested volunteers completed an online assessment to verify their cybersecurity expertise, and Merit sent qualified applicants to the state's volunteer registry. Volunteers who passed a subsequent background joined the MiC3.

In 2016, the state assumed full ownership and operations of MiC3 and hired a part-time manager to oversee the program. This included administering the testing, vetting, and onboarding process; formalizing partnerships with the State Police and National Guard; and expanding awareness throughout the information security community.

When volunteers initially joined the corps, they were placed in one of ten teams, each assigned to one of Michigan's ten "prosperity regions."[2] This team model was based on the desire to have a team that can be easily deployed to any geographical location. As MiC3 grows (with a goal of 200 members), and in recognition of the distributed nature of the cyber environment, and the feasibility of remote access, the state is considering new team models. Future teams may be organized by industry—such as finance, healthcare, energy, etc.—or around skillsets pertaining to the type of attack (e.g. denial of service or ransomware).

Recruitment and Application Process

The MiC3 currently consists of approximately 50 volunteers hailing from the government, academia, business, financial, and healthcare sectors. Membership is open to any Michigan information security professional who can pass a five-phase application process. Applicants must:

- ♦ Hold a basic security certificate;
- ♦ Possess at least two years' experience in information security, preferably security operations, incident response and/or digital or network forensics;
- ♦ Demonstrate basic knowledge of networking and security concepts, as well as basic incident response and forensic skills;

- Secure permission from their employer for time off up to 10 days annually for trainings, exercises, and conferences; and
- Pass a background screening and sign a confidential disclosure agreement (CDA).

Once an applicant successfully becomes a member they receive an official state email address and are eligible for state-funded training. They are also expected to complete certification exams and participate in community service activities. The intent is that the corps provides proactive support for improving the security culture in the community, in addition to reactive support in times of crisis.

Benefits of the MiC3

In addition to increasing and enhancing the state's capacity to respond to cybersecurity incidents, the MiC3 offers several benefits to its members, their employers, and communities.

MiC3 Benefits

Members	**Employers**	**Community**
Access to trainings and certifications	Provides an opportunity for informal information sharing, and development of best practices among industry partners	Ensures small and medium sized organizations have access to a cybersecurity response team
Ability to obtain industry recognized certifications, such as those which satisfy the US Department of Defense's cybersecurity workforce requirements		
Enhancement of professional relationships through networking and collaboration opportunities	Allows an organization to offer a non-monetary incentive to prospective employees by highlighting their partnership with MiC3	
Fulfillment of civic duty and opportunity to work with state police and National Guard		Frees affected persons and entities of potential financial burdens of a cyber incident
Creating and forming the security culture throughout the state	Members can use the skills and trainings they learned through MiC3 at their jobs	

Challenges

Notwithstanding the progress and benefits that MiC3 has made, the program has and continues to face three challenges: Growing Pains; Legal Issues; and Recruitment.

1. *Growing Pains*

   MiC3 confronts challenges that impacts any new organization. First and foremost is ascertaining sufficient funding to not only sustain the program, but to grow it. Half of MiC3's current operating budget goes to training, with the remaining half divided between salary for program staff and program materials. The state now faces the challenge of quadrupling this budget, if not more, to meet a goal of 200 members. An additional challenge to expanding the program is the organizational change that comes with it. The current 50 membership size is equivalent to an NFL football team and can therefore have a team mentality. Yet, expanding to 200 members makes the MiC3 as large, if not larger than some state agencies, bringing with it a host of organizational challenges. MiC3 leaders express concern with maintaining the current "team spirit" or culture, and the need for more full-time management support. Lastly, expanded membership will only exacerbate present difficulties in convening the current group in-person.

2. *Legal Issues*
   Michigan is advancing legislation to assist with associated legal challenges.[3] Specifically, MiC3 members need operational immunity to avoid liability that arise from incident response activities. Second, roles and responsibilities of members with law enforcement personnel and National Guard partners need to be clarified. Lastly, pending legislation would create guidelines for an MiC3 advisory board that would define MiC3 powers and duties. Even with the passage of new legislation, there is still a level of trust and rapport that needs to be established among the private sector community. Although every MiC3 members signs a CDA, private businesses may be reluctant to allow a member(s) onto their network if that member(s) works for a competitor.

3. *Recruitment*
   A recurring issue in the cybersecurity field is hiring professionals who can pass a stringent background check. While some organizations are moving to more lenient security measures, states in general will have to weigh the pros and cons of introducing more lenient background checks. Additionally, MiC3 must consider its bar to entry. Demanding exquisite qualifications will reduce the pool of applicants, while easing requirements could reduce the MiC3 capabilities. MiC3 has dealt with this problem by making the bar to entry moderately difficult, but requires continuous assessment for all MiC3 members.

Recommendations for States

A civilian corps has attracted interest in other states because it can alleviate the current burden of unfilled information security positions in government. More important, it allows the state to assist more entities who fall victim to a cyber attack and to build a greater rapport with their private sector partners. For states interested in developing their own cyber civilian corps, they should consider the following recommendations:

- Identify and convene stakeholders from government, academia, business, financial, and other industry sectors to create the volunteer organization and foster goodwill;
- Establish and maintain executive support—Governor's office, agency heads, and private sector leaders—through a coalition or steering committee to coordinate efforts;
- Leverage existing information security networks within the state to spread word of the corps;
- Engage the higher education community to establish potential internships with the state, which could then be used as a pipeline to the corps;
- Establish memorandum of understandings with cyber ranges to assist in training efforts;
- Identify the resources available to scope how many volunteers can be effectively trained and managed;
- Reach out to cybersecurity training and certification industries to forge partnerships; and
- Work with the legislature to advance any legislation needed to provide immunity or establish roles and responsibilities for the volunteers.

Michael Garcia
Policy Analyst
Homeland Security and Public Safety Division
NGA Center for Best Practices
mgarcia@nga.org

June 2017

NGA would like to thank the State of Michigan for its informational support of this publication.

[1] MiC3 would follow the processes described in the State's Disruption Response Plan. State of Michigan. October 2015. "Cyber Disruption Response Plan." Retrieved from https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

[2] John Karras. August 2014. "TIP Engaged by the Est Michigan COG for Regional Prosperity Strategy." *TIP Strategies*. Retrieved from http://tipstrategies.com/blog/2014/08/tip-engaged-by-east-michigan-cog/

[3] Michigan Legislature. "House Bill No. 4508" Retrieved from http://www.legislature.mi.gov/documents/2017-2018/billintroduced/House/pdf/2017-HIB-4508.pdf