

## INNOVATIVE PRACTICE

### Michigan Cyber Initiatives

May 16, 2016

#### SUMMARY

Michigan's emergency managers and state officials are building public-private partnerships and using grant funding to enhance the state's cyber response capabilities. Initiatives include the Cyber Range, which is training members across the community in cybersecurity response skills; the Michigan Cyber Command Center (MC3), which is enhancing coordination between the state's fusion and the State Emergency Operations Centers; and the Michigan Cyber Disruption Response Plan development, which will help government, industry, and community organizations respond to malicious cyber activity.

#### DESCRIPTION

Since 2012, Michigan has increased the state's cybersecurity workforce response capabilities. The Cyber Range has trained more than 2,900 whole community partners through interactive, virtual training programs. Initially supported with \$365,000 in Homeland Security Grant Program (HSGP) funds, the Cyber Range is a public-private partnership offering in-person and online courses in 14 topics including digital forensics, incident handling, penetration testing, and information systems auditing. Students practice skills through an interactive, virtual exercise—known as Alphaville—that challenges participants to defend a simulated town's network against a team of skilled hackers. Participants may earn certifications through exams accredited by the National Security Agency and Committee on National Security Systems. Moreover, the creation of the Cyber Civilian Corps—a volunteer team of subject matter experts—supports response and recovery activities during a governor-declared state of emergency due to a cyber incident.

Michigan has improved information sharing between state intelligence centers through purchasing information technology equipment with a modest investment of \$4,800 in HSGP funds to support the effort. This equipment is helping the MC3—which organizes the state's cybersecurity criminal investigation, intelligence sharing, mitigation, recovery, and prosecution activities—process cyber threats received by the Michigan Intelligence Operations Center—the statewide fusion center—and coordinate actions with the State Emergency Operations Center. Since its inception, the MC3 has led the investigation of several cyber incidents, 13 of which resulted in criminal prosecution.

With \$75,000 in HSGP funds, Michigan developed a scalable, statewide Cyber Disruption Response Plan to develop action-specific response plans to cyber threats categorized by five levels of severity. Michigan tested the plan through a tabletop exercise with 125 government, industry, and education partners, allocating an additional \$75,000 in funds. The exercise scenario—a cyber breach of sensitive health and banking data in conjunction with a disease outbreak and hacking of State of Michigan infrastructure systems—identified existing cyber response capacities and highlighted the importance of private and public partnerships to improve response capabilities.



Michigan's Cyber Range promotes growth within the cybersecurity workforce pipeline (DTMB)

## REFERENCES

DTMB and MSP, Email correspondence with the FEMA National Preparedness Assessment Division, January 5, 2016.

**DISCLAIMER** *The Lessons Learned Information Sharing Program is a Department of Homeland Security/Federal Emergency Management Agency's resource for lessons learned and innovative ideas for the emergency management and homeland security communities. The content of the documents is for informational purposes only, without warranty, endorsement, or guarantee of any kind, and does not represent the official positions of the Department of Homeland Security. For more information please email [FEMA-LessonsLearned@fema.dhs.gov](mailto:FEMA-LessonsLearned@fema.dhs.gov).*