For press/media contact:

Barbara Hiemstra, WMCSC Co-Chair
Phone: 616-437-5760
Email: wmcybersecurity@kentcountymi.gov

West Michigan Cyber Security Consortium (WMCSC) is Seeing Purple this Month in a Real-Time Hacking Competition on Friday, July 14th

"The Best Defense is an Informed Offense" -Jack Dempsey per Goodreads.com

GRAND RAPIDS - Much of today's news seems to include a cybersecurity twist. How do companies prepare for Cyber incidents? They exercise or practice, as we will at Grand Valley State University's Pew Campus – DeVos Center in Grand Rapids. Sign up today for the 5th annual WMCSC Cybersecurity Exercise to use the Michigan Cyber Range's *Alphaville*. The day-long exercise introduces the Purple Teams. Typically, cybersecurity Teams are Red (offense) or Blue (defense); working together, they are Purple Teams.

Alphaville, developed by Merit Network in Ann Arbor, is a collection of virtual machines simulating information systems that are networked together and assigned varying security levels modeled on how real towns across the country are configured. It exists as part of the Michigan Cyber Range, a secure test bed designed to enable cybersecurity attacks and defense methods in a realistic environment without impacting production network traffic.

The nine Purple Teams will be challenged to capture, secure and defend email servers, web servers, and file systems, using security and hacking tools comparable to the systems found in most businesses today. They will compete against each other hoping to be crowned the winners for "owning" the most systems for the longest time.

The cybersecurity event on July 14 is open to the public; space is limited. Interested attendees must RSVP to wmcybersecurity@kentcountymi.gov by **July 7th**. There is no charge to attend.

About West Michigan Cyber Security Consortium

The West Michigan Cyber Security Consortium (WMCSC) is a multi-jurisdictional, public/private partnership whose purpose is to enhance the prevention, protection, response, and recovery to cybersecurity threats, disruptions and degradation to critical information technology functions. Its membership includes individuals from government, healthcare, law enforcement and private businesses. The group meets quarterly to share information around cybersecurity issues.

About Michigan Cyber Range

The Michigan Cyber Range prepares cybersecurity professionals to detect, prevent and mitigate cyberattacks in a real-world setting. Like a test track or a firing range, the Michigan Cyber Range enables individuals and organizations to conduct "live fire" exercises: simulations that test the detection and reaction skills of participants in a variety of situations. The Michigan Cyber Range also offers certification courses for a number of cybersecurity disciplines, with instruction available on-site and live online. A full training schedule may be found at the Merit Michigan Cyber Range web site: www.merit.edu/cyberrange/

The Michigan Cyber Range is hosted and facilitated by Merit Network in partnership with the State of Michigan and with the sponsorship of Consumers Energy and DTE Energy.

About Merit Network

Merit Network, Inc. is a nonprofit corporation owned and governed by Michigan's public universities. Merit owns and operates America's longest-running regional research and education network. In 1966, Michigan's public universities created Merit as a shared resource to help meet their common need for networking assistance. Since its formation, Merit Network has remained on the forefront of research and education networking expertise and services. Merit provides high-performance networking and IT solutions and professional development to Michigan's public universities, colleges, K-12 organizations, libraries, state government, healthcare, and other non-profit organizations.

For more information: www.merit.edu/