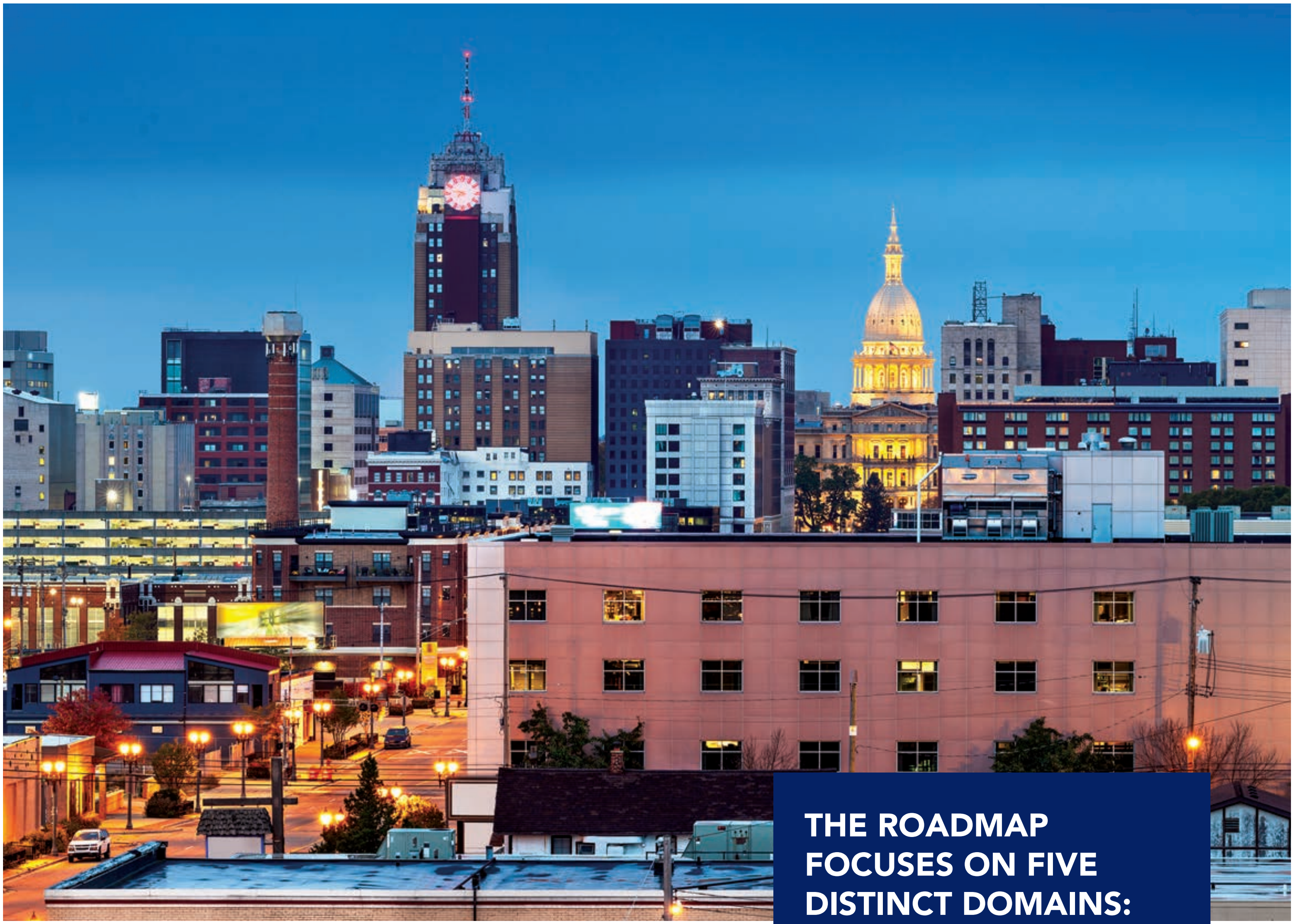
2024 MICHIGAN CYBER ROADMAP

MICHIGAN ECONOMIC DEVELOPMENT CORPORATION

DTMB
Technology, Management & Budget



Michigan has long been considered a national leader in cybersecurity. With a continued focus on whole-of-state cybersecurity, State of Michigan has been creating and refreshing cyber roadmaps and initiatives for over a decade. In late 2023, public and private sector industry leaders across the state engaged in several working sessions and tabletop discussions to develop and create the "2024 Michigan Cyber Roadmap."

Each domain has several initiatives that build upon past successes to enhance Michigan's status as a national leader in cybersecurity. Stakeholders for each domain provided visibility into the current and future state of their respective domains, offering critical insight into how each initiative will be accomplished.

A website is being developed with additional information on the Michigan Cyber Roadmap. The website details key strategic initiatives within this roadmap and will be used as a conduit to assist with collaboration opportunities and help to identify and coordinate initiative champions, funding sources and working groups.

THE ROADMAP FOCUSES ON FIVE DISTINCT DOMAINS:

- **Advanced manufacturing and mobility**
- **Critical infrastructure**
- **Defense organizations**
- **Health care and government**
- **Modernized workforce**

CYBER ROADMAP

There are initiatives that span across all domains, including establishing a unified security operations center (SOC) model, a one-stop portal showcasing all of Michigan's cyber capabilities and a Michigan State Cybersecurity Strategy Forum.

Establishing a unified SOC model will provide a security information and event management (SIEM) solution to level the playing field for entities. Local governments, K–12, higher education and executives will be able to gain awareness of the latest cybersecurity happenings when logs are ingested and alerts are pulled. A unified SOC model will be an affordable offering that allows information sharing between organizations, closing the gap between a zero-day model and a second-day model, and will allow the ability to plug individual SOCs into a central SOC. The SOC services will be available at a discounted rate through the expansion of public and private partnerships that span education, transportation and more, allowing for wider use. The SOC will also allow for the creation of a regional cyber civilian corps, taking the existing program and expanding the volunteer force by providing awareness on cybersecurity from a regional perspective with refreshed initiatives, training and learning opportunities.

Establishing a one-stop portal showcasing all of Michigan's cybersecurity capabilities will provide easy access to the many tools businesses and residents can access from various organizations, cross-linking agency, federal and industry sites. The portal will be marketed to ensure full awareness, use and growth of the site and accompanying resources.

A **Michigan State Cybersecurity Strategy Forum** will connect the dots between risk, resilience, synergy and resources across multidisciplinary fields while connecting stakeholders to find common ground on data sharing, economic development and workforce development. Linking individual sectors will enhance Michigan's security posture and present a united front against evolving threats. The forum will focus on prevention, response and workforce development while proactively encouraging cybersecurity education and awareness. In turn, members will gain knowledge and experience in cybersecurity to further strengthen the digital landscape.

Michigan has accomplished many cybersecurity successes in the last decade. Several resources were launched for public entities and residents, including the Michigan Cyber Partners program, the Michigan Secure App, a risk assessment contract vehicle, and Michigan's implementation of the State and Local Cybersecurity Grant Program. Michigan has also enhanced alignment with high-profile and critical organizations like the Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing and Analysis Center (MS-ISAC) and has continued holding the Michigan Cyber Summit and the Governor's High School Cyber Challenge. Michigan held its first-ever Michigan High School Cyber Summit in 2023, with over 400 high school students from across the state in attendance.

Michigan continues to lead the way in cybersecurity developments. The accomplishments it has already achieved will propel initiatives outlined in the Michigan Cybersecurity Roadmap, helping secure and enhance the digital ecosystem for all Michiganders.

ADVANCED MANUFACTURING AND MOBILITY

CURRENT STATE

Manufacturing processes are becoming increasingly digitized, relying on interconnected networks. To ensure the area remains secure, several initiatives have been implemented, including:

- The Transportation System Management and Operations (TSMO), which emphasizes traffic signal reliability and increased electronic communications, maintenance and development of current system roadside units, prepares for increased electronic communication among vehicles and infrastructure.
- The American Center for Mobility has led collaboration for testing new products, fostering innovation and advancing manufacturing and mobility.
- The increased focus on electric vehicles, charging infrastructure and research to promote sustainable and technologically advanced transportation.
- The wide variety of initiatives hosted at colleges, universities and businesses to increase workforce knowledge and create more jobs:
  - » The Grand Valley Cyber Threat Range provides a safe environment for students and industry to engage in threat exercises and practice training in a secure environment.
  - » The West Michigan Center for Arts and Technology (WMCAT), a teen technology education program, fosters interest and skills in technology and cybersecurity.
  - » Project Patriot provides national veterans with consulting to address professional development, training and skills gaps.
  - » Automation Alley: in partnership with the U.S. Department of Energy, SensCy, Fraunhofer, Grimm and Oakland University, have launched the Cybersecurity Center at Oakland University to strengthen Michigan's cyber resilience
  - » Washtenaw Community College: Advanced Transportation Center, provides education and training in advanced transportation, advanced manufacturing, information technologies and intelligent transportations systems to meet the rapidly developing needs of the mobility workforce.

FUTURE STATE

Approaches to advancing Michigan's manufacturing and mobility sectors are multifaceted, addressing crucial cybersecurity components across development and operations. The integration of new and emerging technologies into process and mobility solutions introduces vulnerabilities and increases the potential of cyber threats. Workforces need to be able to navigate the intricacies of cybersecurity and collaborate with industry partners to establish protocols and standards to secure the ecosystem.

An **Advanced Manufacturing and Mobility Consortium** will improve the relationship and partnership between government and industry in Michigan. The consortium will accelerate appropriate aid to businesses by gathering feedback on opportunities and market direction, enabling Michigan to respond with greater speed and accuracy. These industries will receive a three-part message to inform, increase and educate on cyber resources. Leveraging existing resources and building upon them will further strengthen collaboration, creating an environment where businesses have access to support networks and new generations moving into the workforce have access to cyber training.

A **Cyber Opportunities Connections Center** will use existing resources to provide a more prepared and secured business environment for Michigan by using funding opportunities for enhanced cyber protections. The center will provide a clearinghouse and a tangible tool with opportunity notifications and launch an advocacy campaign to help spread cyber awareness.

Attracting new manufacturing and mobility business to a cyber-secure Michigan will position the state as a cybersecurity hub. The creation and growth of robust partnerships with industry leaders, academic institutions and state and local government will make a world-class knowledge-sharing network that offers businesses access to Michigan's cybersecurity expertise.

CRITICAL INFRASTRUCTURE

CURRENT STATE

Critical infrastructure cybersecurity has several ongoing initiatives that encompass energy and utilities, transportation, water and emergency services, including:

- The Utility Consortium allows companies and regulators to join forces and share non-sensitive, non-competitive information around common threats.
- The Michigan Public Service Commission offers a cyber regulatory framework to establish rules and standards for cybersecurity across sectors.
- The State and Local Cybersecurity Grant Program allows state and local public entities to receive funding opportunities to secure organizations and increase the state's security posture.
- The Chief Security Officer Kitchen Cabinet is a membership-required meeting with information sharing between multiple intelligence, cybersecurity and economic development areas to proactively address cyber challenges.

FUTURE STATE

Critical infrastructure continues to evolve with increased reliance upon interconnected digital systems. The interconnected nature of these systems creates a complex structure that is vulnerable to cyber threats, which could impact public safety, economic stability and effective functions across the state. Proactive cybersecurity strategies and initiatives to safeguard reliable essential services are necessary for resilience.

Establishing cybersecurity requirements in the Michigan High-Speed Internet Office will ensure that high-speed internet infrastructure is secure while connecting unserved and underserved individuals, businesses and community organizations. Those who apply for Broadband, Equity, Access, and Deployment (BEAD) program funds to support the construction of high-speed internet infrastructure will need to meet cybersecurity requirements. Increasing personal cybersecurity skills will help digital equity across the state, as outlined in the state digital equity plan.

Securing electric vehicle (EV) charging stations and distributed energy resources will ensure greater alignment within the sector, to secure energy resources across plant, third-party and consumer-owned locations. Collaboration with utilities will assess initiatives already in progress and identify cybersecurity requirements for electric vehicle charging stations and distributed energy resources. Identifying cybersecurity requirements for these areas will ensure that sites are internet-enabled and that vendors are properly certified.

Securing traffic signals and securing large highway water pumps will ensure that systems are safe and secure. All new, upgraded traffic signals must now be smart signals that allow for the change signal phase and timing to be done remotely through a centralized system. As cities, villages and counties become able to operate such systems, connections must be secured, with full understanding and documentation to ensure security and public safety. The shift from large water removal pumps to internet-enabled pumps will require that support vendors perform system security plans to ensure systems are safe and secure.

A **drinking water cybersecurity assessment** will improve cybersecurity in the water and wastewater systems sector, ensuring stability and health for Michigan and the nation. It will use existing resources from high-profile agencies and organizations to emphasize cybersecurity best practices while providing training for small or critical infrastructure providers. It will also provide a template for water sector cybersecurity assessments to protect systems.

DEFENSE ORGANIZATIONS

CURRENT STATE

Defense organizations and systems are constantly exposed to threats, resulting in several ongoing initiatives to help secure the current state, including:

- Tabletop exercises demonstrate the importance of cybersecurity when it is not always visible. Exercises are available for defense and manufacturing organizations, as well as for civilians through a partnership with the Michigan State Police (MSP).
- The Metro Detroit Regional Vehicle Cybersecurity Institute is a consortium designed to expand and enhance the cybersecurity engineering workforce. It was established with funds from the Department of Defense to the University of Detroit Mercy through the Griffiss Institute's Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ (VICEROY) program.
- The cyber systems integration lab focuses on conducting penetration testing and analysis of vehicle systems and can operate at both secret and unclassified levels.
- The Michigan Department of Transportation (MDOT) and Ground Vehicle Systems Center cooperative agreement allows collaboration regarding towers and autonomy while exploring truck communication in convoys with person centric identity services (PCIS) technology.
- The Army and Air National Guard collaborate each month to produce a cyber update brief for the adjutant general.
- Industry partnerships that leverage Michigan's unique industry and manufacturing capabilities remain critical to secure defense organizations. This includes the Kelly Johnson Joint All-Domain Innovation Center, which promotes partnerships between the Michigan National Guard (MING), industry, DoD research agencies, and academia.

FUTURE STATE

Defense organizations and systems are becoming increasingly interconnected, relying on complex networks and digital infrastructure to safeguard against constantly evolving threats. Adversaries are constantly evolving their tactics to access systems. As a result, defense organizations need to leverage innovative technologies, foster collaboration and invest in R&D to create adaptive systems that can quickly respond and stay ahead of threat actors.

Creating a Connected Vehicle Cybersecurity Center of Excellence will foster collaboration and share cutting-edge concepts and information. The center will drive innovation in safeguarding connected vehicles from cyber threats, offering an automated vehicle cybersecurity integration center, a space for collaborative testing between public and private partners and unified security standards for the trucking national supply chain. The center will also focus on the exchange of data between vehicles, ships and critical factors of national defense to better understand and protect the movement of troops and goods.

Intrusion Detection and Prevention Systems (IDPS) for Ground Vehicles will explore the potential for applications beyond the military, as there is a high degree of commonality between commercial and military automotive systems. Projects have already been completed to develop IDPS for military ground vehicles.

The creation of a **next-generation Michigan Automotive Cybersecurity Center** will build a strong foundation for a secure and interconnected automotive landscape. The center will contribute to the development and implementation of workable cryptographic systems, ensuring that data transmission within vehicles and across the global infrastructure remains safeguarded. The focus on cyber-physical systems will uphold the integrity of the technology that powers and protects our world, furthering Michigan's strong ties to the automotive industry.

The **development and formalization of a strategic convening or consortium-based group with the ability to partner with federal, state, local, industry or other experts** will strengthen relationships and partnerships between government and industry, allowing for information sharing on cyber developments, emerging threats and actions taken to help secure organizations. The group will increase collaboration between entities and provide appropriate contacts and available resources to help secure the cyber environment.

Promoting encryption capabilities for radios that lack the capacity to have true encrypted communications on the local level at any given time will ensure that communications are secure. Encryption will prevent sensitive information from unauthorized use, ensuring that the communications and orders shared via radio are received only by the intended users.

Widening statewide cyber defense and emergency management incident response exercises will increase preparedness and knowledge in a cyber emergency. Developing and conducting exercises will give responders full awareness before an emergency, incident or event occurs, allowing for a better, more effective action and response. The existing cyber disruption response plan will be utilized, expanding the scope of tabletop exercises while exploring how to increase the size of resources.

HEALTH CARE AND GOVERNMENT

CURRENT STATE

Health care and government sectors safeguard sensitive information and provide the integrity of essential services by implementing several initiatives, including:

- The Michigan Healthcare Cybersecurity Council, a collection of Michigan health care chief information security officers with integration from federal organizations, gather to share strategies and collaborate against common threats.
- The Health Security Operations Center, unique to Michigan, fosters a statewide culture of collaboration by creating standardized playbooks and lessons learned and providing trained incident response services.
- The MISecure task force, organized by the Michigan Education Technology Leaders, has developed a guide to help Michigan K–12 school districts identify and improve cybersecurity practices while offering resource materials.
- The Michigan Cyber Summit, led by the Michigan Department of Technology, Management & Budget (DTMB), brings together cybersecurity professionals for sessions and networking related to the latest cyber topics.
- Several government initiatives have helped strengthen Michigan's current state, including Michigan Cyber Partners, a collaboration between divisions across state government and local public entities to strengthen and promote cybersecurity resources and best practices.

FUTURE STATE

Health care and government sectors are frequently targeted by cybercriminals due to their data, size and reliance on technology. Implementing innovative cybersecurity measures that focus on advanced threat detection, robust data encryption and resilient infrastructure is necessary to secure the operations and handling of sensitive information across health care and government. These innovations in cybersecurity will foster public trust by ensuring the protection of citizen data and privacy and the availability and readiness of essential services.

Providing education for the general public will strengthen cyber knowledge and create apprenticeship programs that provide next-generation tools to secure the digital ecosystem. This initiative create a strong public understanding of staying secure in the growing digital ecosystem while using cybersecurity industry terminology that is based on a foundational consumer interest.

MODERNIZED WORKFORCE

CURRENT STATE

Modernizing the workforce is essential to securing Michigan's digital ecosystem. Several programs and initiatives have been implemented, including:

- Centers of Academic Excellence across Michigan, managed by the National Security Agency (NSA) and the Department of Homeland Security (DHS), create a collaborative cybersecurity education program with colleges and universities.
- Outreach for K–12 offers cyber teacher certifications to improve STEM education and talent development.
- The CyberPatriot Program serves all of Michigan, inspiring students to consider careers in cybersecurity, technology and engineering by hosting virtual cybersecurity competitions and summer camps for students.
- Federal partnerships and initiatives allow for youth apprenticeships in cybersecurity. The National Science Foundation (NSF) funds scholarships in cybersecurity and the Department of Education funds a partnership between Oakland University and Automation Alley to host a cybersecurity center for energy systems.
- Programs like NPower create pathways to digital careers for military veterans and young adults through various trainings and mentorships. Other programs throughout Michigan have allowed those involved in cyber to form connections and increase their cyber knowledge, including the Michigan Council for Women in Technology, the West Michigan Cybersecurity Consortium and Latinas in Cyber.
- Michigan's CyberAuto, CyberTruck and CyberMedical Challenges highlight the state's leadership in cybersecurity and workforce training, helping teams identify embedded systems cybersecurity trends and develop talent in a new technical discipline while creating a community of interest.

FUTURE STATE

Investing in educational programs, specialized training initiatives and partnerships with cyber-focused institutions will continue to help the state develop a skilled workforce. The workforce's interconnected and mobile nature requires strong cybersecurity measures to prevent disruption, protect information and uphold the state's reputation as a reliable and secure hub for modern business operations. A strategic expansion of the workforce will assist in adapting to the changing cyber landscape and maintaining a secure environment.

Enhancing the Michigan Cybersecurity Education Centers of Excellence will leverage existing cybersecurity programs and transform them into a cost-effective training and education consortium. All currently certified cybersecurity trainings and education programs will be one focused effort dedicated to cybersecurity awareness, training and education for all sectors of the economy. The initiative will establish an uninterrupted development process for students, creating a pathway from high schools to colleges and universities to industry stakeholders. The centers will expand the workforce by increasing the number of students entering cyber education and career pathways.

Strengthening grants and educational opportunities will encourage careers in cybersecurity by showcasing opportunities to become engaged. Using educational networks to incentivize professional learning opportunities with grants for cybersecurity will reach thousands of youths and hundreds of educators. Existing education and internship programs for students will be tailored and expanded to build out opportunities and provide a wider range of interns. Michigan's government will use the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Framework to enhance the workforce, providing the building block terminology needed to perform cybersecurity work.

Increasing awareness of cyber careers through advertising will attract more workers, and more emphasis on engaging students of all ages will showcase that the field is for everyone. Encouraging students to become interested in cybersecurity will involve additional teacher support, education and implementation of after-school programs. Further strengthening partnerships with community organizations and community colleges will help create and maintain programs for teacher education to address the shortage of cyber educators.

Creating a cybersecurity apprenticeship program and identifying networking opportunities will modernize the workforce. The apprenticeship program will include various cyber pathways, providing direct training and experience to help apprentices thrive in the work environment. Networking opportunities will help connect the existing and future workforce with opportunities to showcase their talent while creating connections that will provide valuable insight into the cyber field.

CONCLUSION

The integral role of cybersecurity in daily life requires attention, awareness and preparation to ensure the digital ecosystem is secure. Michigan's Cyber Roadmap will ensure the state's most critical areas remain secure over the next several years. Focusing on the five domains of advanced manufacturing and mobility, critical infrastructure, defense, health care and government and modernized workforce will ensure that each domain is properly addressed and secured in a constantly changing landscape.

In 2011, the first publication of the "Michigan Cyber Initiative: Defense and Development for Michigan Citizens, Businesses and Industry" was released, providing a blueprint for protecting the cyber landscape. In 2015, the initiative was refreshed and renamed to "Michigan Cyber Initiative 2015, Leading the Nation: An interagency, public/private collaboration" and built upon the original initiative while driving Michigan to the future of cybersecurity.

The 2024 refresh of the initiative, Michigan's Cyber Roadmap, builds upon the 2015 release while advancing Michigan's continued focus on whole-of-state cybersecurity with clear initiatives and goals to help secure the state and ecosystem. The roadmap will help Michigan embark on new cyber developments, expand upon existing offerings and connect professionals, leaders and the current and future workforce with the tools needed to stay secure.

Michigan is a leader in cybersecurity despite the frequently changing digital ecosystem. The **Michigan Cyber Roadmap** will help ensure that Michigan remains at the forefront by building upon existing content and creating new opportunities to strengthen the overall cyber posture of the state, benefiting industry, businesses, residents and the state as a whole.

The Michigan Cyber Roadmap was developed through cross-agency collaboration. Led by the Michigan Economic Development Corporation (MEDC) and DTMB, several agencies were involved, including the Department of Environment, Great Lakes, and Energy (EGLE), Michigan Department of Health and Human Services (MDHHS), Department of Labor and Economic Opportunity (LEO), Michigan Department of Education (MDE), MDOT, MSP and MING. Industry leadership and collaboration also played a key role in developing the roadmap, providing critical insight on how to best secure their domain. This collaboration allowed for many ideas to be shared, resulting in several new initiatives taking shape and becoming priorities for upcoming years.

APPENDIX A: LIST OF PARTICIPANTS

Laura Clark
Chief Information Officer/
State of Michigan Department
of Technology, Management &
Budget (DTMB)

Jayson Cavendish
Chief Security Officer/
State of Michigan DTMB

Mark Ignash
Strategic Initiatives & Ecosystem
Development Director/Michigan
Office of Defense and Aerospace
Innovation (ODAI)

Dan Lohrmann
Presidio

Sarah Tennant
Senior Sector Development
Director & Cyber Advisor/MEDC

Dillon Trombly
Chief of Staff/State of Michigan
DTMB

Laura Wotruba
Director of Communications/
State of Michigan DTMB

Critical Infrastructure Domain

Jim Beechey
Consumers Energy

Rod Davenport
Oakland County

Andy Esch
Michigan Department
of Transportation

T.J. Fields
Oakland Country

Frank Garcia
Great Lakes Water Authority

Steve Herrin
DTE Energy

Ryan McAnany
Michigan Public Service
Commission (MPSC)

Rex Menold
State of Michigan DTMB

Vern Meyers
Lansing Board of Water & Light

Alexander Morese
Michigan Public Service
Commission (MPSC)

Brad Pagratis
Michigan Department of
Environment, Great Lakes,
and Energy (EGLE)

Brian Pillar
State of Michigan DTMB
Supporting MDOC, MSP, DMVA

Dan Rainey
City of Detroit Water and
Sewerage Department

Jessica Randall
Michigan High-Speed
Internet Office

Jesse K Reisman
DTE Energy

Andrew Wcisel
Consumers Energy

Advanced Manufacturing and Mobility Domain

Kelly Bartlett
Michigan Department of
Transportation (MDOT)

Tim Beck
Kent County

Karl Heimer
Principal/Heimer
& Associates LLC

Cynthia Hutchison
US Center of Advanced
Manufacturing

Manny Rosales
State of Michigan DTMB

Scott Taber
Michigan Small Business
Development Center

Ingrid Tighe
Michigan Manufacturing
and Technology Center

Jennifer Tisdale
Grimm

Jen Wangler
The Right Place

APPENDIX A: LIST OF PARTICIPANTS

Modernized Workforce Domain

Roger Blake
Merit Network Inc.

Kim Crawford
Division Director/
State of Michigan

Tiziana Galeazzi
(AG, GOV, LEO, MDOT)/
State of Michigan DTMB

Ryan Hundt
Michigan Works! Association

Bhavani Koneru
Oakland University

Barb Land
Square One Education Network

Al Lecz
Washtenaw Community College

Gina Loveless
Michigan Department
of Education & MiLEAP

Matt McMahon
Michigan Education
Technology Leaders (METL)

Michael Sauer
Upper Peninsula Cybersecurity
Institute at Northern Michigan
University

Megan Schrauben
State of Michigan
MiSTEM Network

Tamara Shoemaker
Cyber Security Education,
Training, and Awareness; K–12
Cyber Security Education, MCISSE
CyberPatriot Program

Milos Topic
Grand Valley State University

Ashley Wisniewski
Michigan Community
College Association

Defense Organizations Domain

Lt. Col. John Brady
Michigan Air National Guard

Ryan Cross
State of Michigan OIP

Aaron Dupre
Michigan Security Operations
Center DTMB

Joe Gothamy
U.S. Army DEVCOM Ground
Vehicle Systems Center (GVSC)

Maj. Shawn Hatfield
Michigan Air National Guard

Jeff Jaczkowski
U.S. Army DEVCOM Ground
Vehicle Systems Center (GVSC)

Daniel Lorenz
Department of Homeland Security

Col. Robert Maciolek
Michigan Army National Guard

Brad McNett
U.S. Army DEVCOM Ground
Vehicle Systems Center (GVSC)

Vicky Rowinski
Macomb County Department of
Planning & Economic Development

Marc Shepard
General Dynamics Land
Systems (GDLS)

Phil Smith
U.S. Army DEVCOM Ground
Vehicle Systems Center (GVSC)

Col. Raymond Stemitz
Michigan Army National Guard

Health care and Government Domain

Bob Bacigal
Amerisure Insurance
& CSO Kitchen Cabinet

Nathan Buckwalter
State of Michigan DTMB

Trent Carpenter
Sparrow Health System
& CSO Kitchen Cabinet

D/F/Lt. James Ellis
Michigan State Police; Michigan
Cyber Command Center

Betsy Freeman
Radius Advisory Group LLC

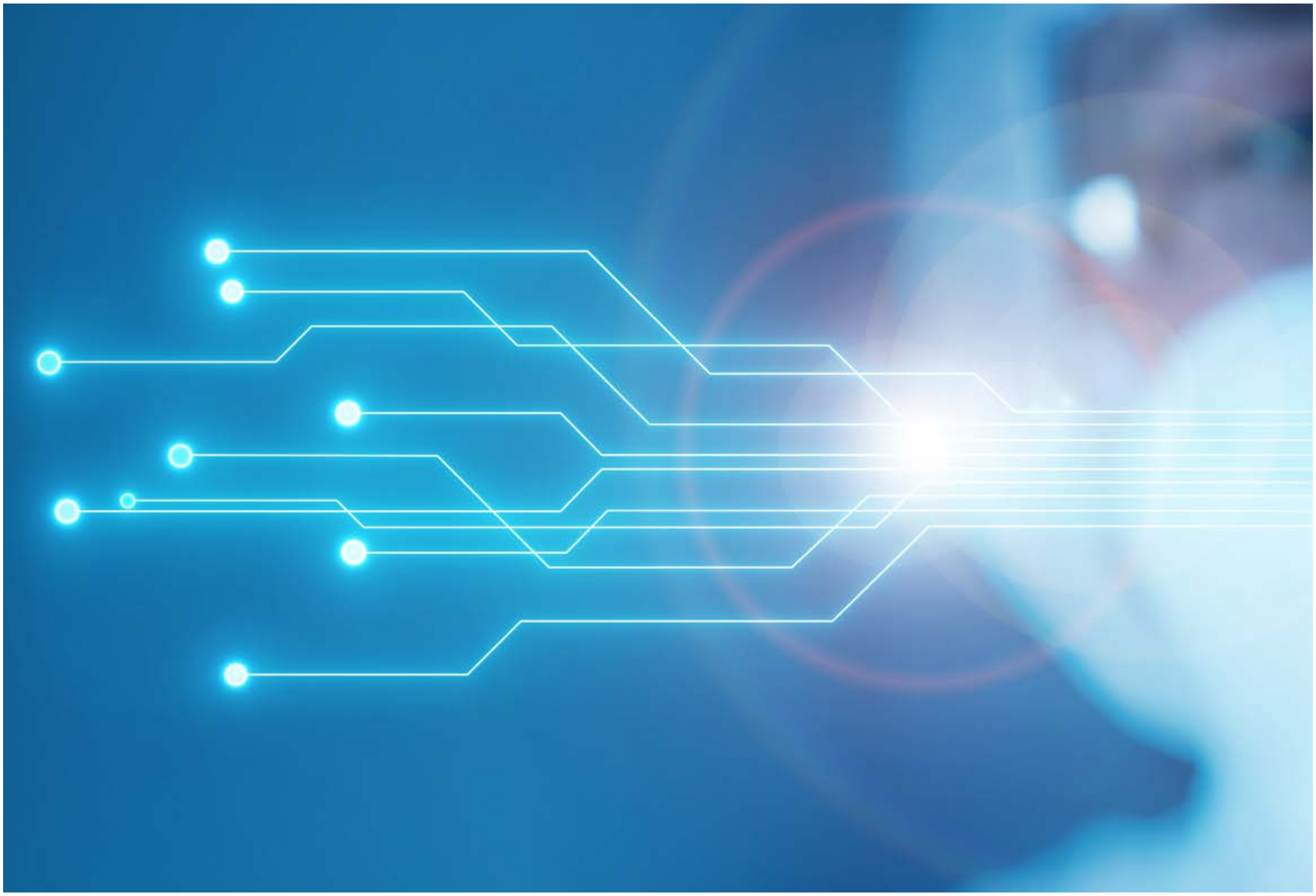
Ashley Gelisse
Michigan Medicine

Luke Otten
Munson Healthcare

Greg Sieg
Michigan Medicine & Michigan
Healthcare Cybersecurity Council
(MiHCC)

Art Thompson
City of Detroit

Tony Weber
State of Michigan Department
of Health and Human Services
(DHHS)



DISCOVER MORE

www.michiganbusiness.org

For more information, please contact:
tennants@michigan.org

MICHIGAN ECONOMIC DEVELOPMENT CORPORATION

DTMB Technology, Management & Budget