

# CIP Four-Year Strategic Plan

Fiscal Years 2024 - 2027

Office of the Chief Security Officer  
Cybersecurity and Infrastructure Protection  
Michigan Department of Technology, Management & Budget

## Mission Statement

Enable the business to function securely while making security easier for customers and harder for hackers.

## Vision Statement

Cybersecurity and Infrastructure Protection (CIP), operating as Business Services, Identity and Architecture (IA), Michigan Security Operations Center (MiSOC), Office of Infrastructure Protection (OIP), and Risk Compliance and Delivery (RCD), will bring a compassionate and empathetic approach to provide digital and infrastructure security services to our customers within state employment, state agencies, and the public by delivering world-class services and providing great customer service.

## Goals

CIP division-wide goals map to the DTMB strategic plan and DTMB IT strategic initiatives to ensure alignment with the overall strategic mission of DTMB.

## Chief Security Officer Objectives

- Reconcile tools used across the divisions to track compliance with DTMB policy, standards, and procedures to ensure planning for lifecycle events, such as authority to operate (ATO), contract renewals, and potential migrations to new products, are planned and managed in advance of end of life and end of contract situations.
- Ensure a DTMB and CIP best practices guide is created that informs employees and contractors of how Michigan government functions and details their role as a member of CIP.
- Oversee the Michigan Cybersecurity External Engagements services, including Michigan's State and Local Cybersecurity Grant Program (SLCGP), CSO Kitchen Cabinet, MiCyberCorps, Michigan Cyber Partners, Cybersecurity Resource Hub, Michigan Secure App, Michigan Cyber Summit, Governor's High School Cyber Challenge, elections security monitoring, as well as other symposiums,

summits, speaking engagements, and outreach across CIP.

## Business Services

- Provide financial planning, purchasing, analysis, and reporting of the budget to CIP division directors.
- Provide human resources support and continue to streamline and implement workflows that will further improve all HR related processes.
- Ensure onboarding and offboarding procedures are created that assist employees and contractors be successful beyond day one with topical onboarding and training plans by work role and duties.
- In partnership with DTMB Communications, consistently provide useful and clear communications to internal and external audiences on a variety of topics relating to CIP.
- Continue to support CIP reporting through the growth of the CIP Data Analytics Program (CDAP) and support other CIP divisions with controlled data sharing and automation services using low-code/no-code systems development.
- Develop a CIP Student Services program to support workforce development within DTMB.
- Introduce a CIP Business Analysis service to support division area project management.
- Provide oversight and onsite management of the CIP assigned Enterprise Portfolio Management Office (EPMO) staff to drive efficiencies within associated EPMO processes and improve the effectiveness of project delivery.

## Identity and Architecture

- Continue to support implementation of the MiLogin Roadmap.
- Provide support for security liaisons, MiSOC, bid solicitations, enterprise architecture, and cloud adoption in compliance with existing and new policies, standards, and procedures.
- Continue to grow adoption of the Secure Application Development Lifecycle (SADLC) and related services in support of Zero Trust



## Architecture and Development Security Operations (DevSecOps) best practices.

### Michigan Security Operations Center

- Develop a cybersecurity centric strategy and multiyear plan to take advantage of innovations within security automation, cloud services, and artificial intelligence (AI) to keep pace with and scale our identification, detection, prevention, response, and recovery capabilities to prepare ourselves for the future.
- Seek opportunities to expand usage of existing and new tools in support of Zero Trust Architecture principles that enforce just-in-time access control provisioning and deprecate reliance on static implicit trust-based access controls, in which these systems include secure service edge platforms and extended managed detection and response tools.
- Establish an affordable public-private partnership based unified SOC model offering to provide a security information and event management (SIEM) capability targeting local governments, K-12, and higher education along with enabling a regional cyber civilian corps.

### Office of Infrastructure Protection

- Manage the emergency services, building access, and building security services necessary for state infrastructure to provide safe and secure working environments.
- Manage the enterprise security awareness and training program, plan tabletop exercises, and lead continuity planning across DTMB.
- Develop a division wide workforce development strategy, plan, and operating model, based on the industry recognized NICE framework<sup>1</sup> and tailored to CIP, that enables role-based career pathways and growth opportunities.
- Implement a division wide training program based on the workforce development strategy.

### Risk Compliance and Delivery

- Continue efforts to streamline and improve the Michigan Security Accreditation Process (MiSAP) automation workflows to increase understanding of

and reduce risk across all State of Michigan applications.

- Monitor and maintain the Information Technology Information Security policies and supporting standards in alignment with federal and industry standard regulatory frameworks while collaborating with the policy management cross functional review team (CFRT).
- Provide support to agencies in gathering relevant control evidence during the MiSAP process and the Internal Control Evaluation (ICE) audits. Guide agencies in achieving successful results in various audits and federal compliance assessments of their programs.
- Establish consistent communication with agency security officers, business relationship managers, and agency IT liaisons to provide them information from other CIP divisions about the status and operational risks carried within the business applications they utilize to serve their customers to include vulnerabilities, incident response liaison with MiSOC, and MiSAP plan of action and milestones (POAM) management.
- Evolve the third party risk management capability of MiSAP to include real time alerts of vendors and partners that are at risk of a cyberattack or have been compromised resulting in possible risk to the State of Michigan's computing environment.

<sup>1</sup><https://niccs.cisa.gov/workforce-development/nice-framework>