
# State and Local Cybersecurity Grant Program (SLCGP)

2024

Michigan's Statewide Interoperable Communications Conference

Michelle McClish

State Assistant Administrator,
External Engagements Lead
Michigan Cybersecurity | Michigan Cyber Partners

February 29, 2024

# State & Local Cybersecurity Grant Program (SLCGP) –What Is This?

- Infrastructure Investment & Jobs Act (IIJA) Congress Establishes SLCGP
- 1$ Billion to be awarded over a 4-year grant life-cycle
- Administered by FEMA & CISA
- Administered locally by MSP/EMHSD and DTMB Michigan Cybersecurity
- Overall Goal : To provide funding to SLTTs to address cybersecurity threats to SLTT owned or operated information systems

# SLCGP Grant Lifecycle

| |
|---|
| **1st Year \| FY2022** |
| **Objective 1** |
| 48 Month Performance & Spend Period - September 2022 – September 2026 |
| **2nd Year \| FY2023** |
| **Objective 2** |
| 48 Month Performance & Spend Period - September 2023 – September 2027 |
| **3rd Year \| FY2024** |
| **Objective 3** |
| 48 Month Performance & Spend Period - September 2024 – September 2028 |
| **4th Year \| FY2025** |
| **Objective 4** |
| 48 Month Performance & Spend Period - September 2025 – September 2029 |

# SLCGP Grant Lifecycle

| | | | |
|---|---|---|---|
| **1st Year \| FY2022** | | | |
| **2023** | **2024** | **2025** | **Sept 30, 2026** |
| **2nd Year \| FY2023** | | | |
| **2024** | **2025** | **2026** | **Sept 30, 2027** |
| **3rd Year \| FY2024** | | | |
| **2025** | **2026** | **2027** | **Sept 30, 2028** |
| **4th Year \| FY2025** | | | |
| **2026** | **2027** | **2028** | **Sept 30, 2029** |

We Are Here

# SLCGP Michigan Allocation

## Grant Year 1

$4,775,415

- FY2022 – Michigan SLCGP Allocation

## Grant Year 2

$9,609,530

- FY2023 – Michigan SLCGP Allocation

## Grant Year 3

$300M (TBD)

- FY2024 - Michigan SLCGP Allocation

## Grant Year 4

$100M (TBD)

- FY2025 Michigan SLCGP Allocation

# SLCGP FY2022 Priorities

## With the FY 2022 SLCGP, recipients were directed to accomplish the following

1. Establish a Cybersecurity Planning Committee
2. Develop Statewide Cybersecurity Plan
3. Use SLCGP Funds to implement or revise a state-wide Cybersecurity Plan

## Michigan’s Progress in FY2022 Priorities

1. SLCGP Planning Committee Established
2. Approved Cybersecurity Plan
3. Participation Survey
4. Education & Outreach for Plan Enhancement
5. Identify & Support Cyber Projects

# SLCGP Objectives

**The goal of SLCGP is to assist SLT governments with managing and reducing systemic cyber risk.**

- **Objective 1:**
  Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

- **Objective 2:**
  Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

- **Objective 3:**
  Implement security protections commensurate with risk.

- **Objective 4:**
  Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

# SLCGP Objective Outcomes

## Objective 1 - Develop & Establish Appropriate Governance Structures

1

**Governance Structure Development:** State and local government entities are encouraged to develop and establish governance structures specifically tailored to cybersecurity management. These structures may include cybersecurity committees, task forces, or dedicated cybersecurity offices responsible for overseeing cybersecurity initiatives, policies, and procedures.

**Cybersecurity Plan Development:** Objective 1 emphasizes the development, implementation, or revision of comprehensive Cybersecurity Plans. These plans outline strategies, policies, and procedures for managing cybersecurity risks, responding to incidents, and ensuring the continuity of operations in the event of a cyber incident or disruption.

**Risk Management Frameworks:** Organizations should adopt risk management frameworks to guide the development of their Cybersecurity Plans. Frameworks such as the NIST Cybersecurity Framework or ISO 27001 provide structured approaches to identifying, assessing, and mitigating cybersecurity risks, helping organizations establish effective governance structures.

**Incident Response Planning:** Objective 1 includes provisions for the development and implementation of incident response plans as part of Cybersecurity Plans. These plans outline procedures for detecting, responding to, and recovering from cybersecurity incidents, ensuring that organizations can effectively manage and mitigate the impact of security breaches.

**Continuity of Operations Planning:** Organizations should integrate continuity of operations planning into their Cybersecurity Plans to ensure resilience in the face of cyber incidents. This involves identifying critical assets and functions, establishing backup and recovery mechanisms, and developing strategies to maintain essential services during and after a cyber incident.

**Stakeholder Engagement:** Objective 1 emphasizes the importance of engaging stakeholders from across the organization in the development and implementation of Cybersecurity Plans. This includes senior leadership, IT personnel, legal and compliance teams, and other relevant stakeholders to ensure buy-in and alignment with organizational goals and priorities.

# SLCGP Objective Outcomes

## Objective 2 - Understand Cybersecurity Posture & Areas For Improvement

2

**Evaluation of Security Controls:** Objective 2 emphasizes the evaluation of existing security controls to determine their effectiveness in mitigating cybersecurity risks. Organizations should assess whether security controls are properly configured, adequately implemented, and capable of addressing current and emerging threats.

**Structured Assessments:** State and local government entities should conduct structured cybersecurity assessments to gain insight into their overall security posture. This may involve using standardized frameworks, such as the NIST Cybersecurity Framework or the CIS Controls, to assess cybersecurity maturity, identify gaps, and prioritize areas for improvement.

**Risk Identification:** Objective 2 involves identifying and prioritizing cybersecurity risks based on the results of testing, evaluation, and assessments. Organizations should assess the likelihood and potential impact of cybersecurity threats to their systems, data, and operations to effectively prioritize remediation efforts.

**Gap Analysis:** Organizations should perform gap analysis to compare their current cybersecurity posture against industry standards, best practices, and regulatory requirements. This helps identify areas where the organization falls short of desired security objectives and informs the development of remediation strategies.

**Remediation Planning:** Based on the findings of testing, evaluation, and assessments, state and local government entities should develop comprehensive remediation plans to address identified vulnerabilities, weaknesses, and gaps in cybersecurity defenses. Remediation plans should prioritize high-risk areas and establish clear timelines and responsibilities for implementation.

**Continuous Improvement:** Objective 2 underscores the importance of a culture of continuous improvement in cybersecurity. Organizations should regularly review and update their cybersecurity strategies, policies, and procedures based on lessons learned from testing, evaluation, and assessments to adapt to evolving threats and changes in the organizational environment.

# SLCGP Objective Outcomes

## Objective 3 Implement Security Protections Commensurate with Risk

3

**Risk Management:** Based on the results of the risk assessment, organizations should develop risk management plans to mitigate identified risks effectively. This may involve implementing a combination of technical controls, administrative measures, and security safeguards to reduce risk exposure to an acceptable level.

**Security Controls Implementation:** Objective 3 emphasizes the implementation of security controls and measures that are proportionate to the level of risk identified during the risk assessment process. This may include measures such as access controls, encryption, intrusion detection systems, and security monitoring tools.

**Security Policies and Procedures:** Organizations should establish clear cybersecurity policies, procedures, and guidelines that reflect the risk management decisions made during the risk assessment process. These policies should outline security requirements, responsibilities, and expectations for personnel to ensure consistency in security practices.

**Continuous Monitoring and Review:** Objective 3 highlights the importance of ongoing monitoring and review of security controls to ensure their effectiveness in mitigating cybersecurity risks. Organizations should regularly assess and update their security posture in response to evolving threats, vulnerabilities, and changes in the organizational environment.

**Incident Response Preparedness:** Organizations should develop and maintain incident response plans to enable a swift and coordinated response to cybersecurity incidents. This involves defining roles and responsibilities, establishing communication protocols, and conducting regular exercises to test incident response capabilities.

**Resource Allocation:** Objective 3 recognizes the need for organizations to allocate resources effectively to implement security protections commensurate with risk. This may involve investing in cybersecurity technologies, training and awareness programs, and hiring skilled personnel to support cybersecurity initiatives

# SLCGP Objective Outcomes

## Objective 4 –Organization Personnel are Appropriately Trained in Cybersecurity

4

**Training Needs Assessment:** Organizations are encouraged to conduct a thorough assessment of the cybersecurity training needs of their personnel. This involves identifying the knowledge and skills required to fulfill their cybersecurity responsibilities effectively.

**Training Program Development:** Based on the training needs assessment, organizations should develop comprehensive cybersecurity training programs tailored to the specific roles and responsibilities of their personnel. These programs may include a combination of classroom training, online courses, workshops, and hands-on exercises.

**Role-Based Training:** Training programs should be designed to address the unique cybersecurity requirements of different roles within the organization. For example, IT administrators may require training on network security and system administration, while non-technical staff may need awareness training on phishing scams and social engineering tactics.

**Technical and Non-Technical Training:** Objective 4 recognizes that cybersecurity training needs vary among personnel, with some requiring technical skills and others needing a broader understanding of cybersecurity concepts. Training programs should cater to both technical and non-technical audiences, ensuring that all personnel receive the necessary knowledge and skills to contribute to cybersecurity efforts.

**Continuous Learning and Development:** Objective 4 emphasizes the importance of ongoing learning and professional development in cybersecurity. Organizations should provide opportunities for personnel to stay updated on the latest cybersecurity trends, technologies, and best practices through continued education, certifications, and participation in industry events.

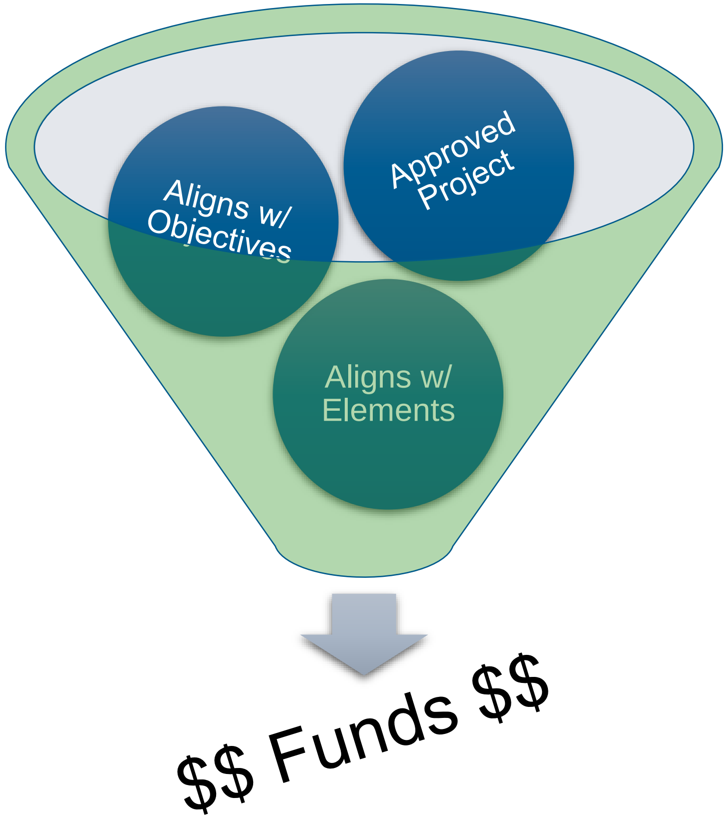
**Performance Evaluation:** Organizations should establish mechanisms to assess the effectiveness of cybersecurity training programs and evaluate the cybersecurity competency of personnel. This may involve conducting knowledge assessments, skills testing, and simulated exercises to measure proficiency and identify areas for improvement.

# Statewide Cybersecurity Plan

- Addresses 4 Grant Objectives
- Addresses 16 Required Elements
- Can be updated anytime - Required to be updated in Year 3
- Cybersecurity Plan is Overarching Strategic Statewide
- Grant Projects for funding must align with the Plan, Elements, & Objectives

**Key Cybersecurity Best Practices - Required Element #5**

- Implement multi-factor authentication
- Implement enhanced logging
- Data encryption for data at rest and in transit
- End use of unsupported/end of life software and hardware that are accessible from the Internet
- Prohibit use of known/fixed/default passwords and credentials
- Ensure the ability to reconstitute systems (backups)
- Migration to the .gov internet domain



# The Cybersecurity Plan – Required Elements

## 16 Required Plan Elements -

**There is NO good way to display this information - But its here for you to read later**

- Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

# The Cybersecurity Plan – Required Elements

## 16 Required Plan Elements -

- Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.
    - Implement multi-factor authentication
    - Implement enhanced logging
    - Data encryption for data at rest and in transit
    - End use of unsupported/end of life software and hardware that are accessible from the internet
    - Prohibit use of known/fixed/default passwords and credentials
    - Ensure the ability to reconstitute systems (backups); and
    - Migration to the .gov internet domain
- Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

# The Cybersecurity Plan – Required Elements

## 16 Required Plan Elements -

- Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.
- Distribute funds, items, services, capabilities, or activities to local governments.

# SLCGP Road Map -16 Required Elements - A Better Way to Display - SLCGP (cisecurity.org)

https://www.cisecurity.org/ms-isac/slcgp

CIS Center for Internet Security
Creating Confidence in the Connected World.

CIS Hardened Images   Support   CIS WorkBench Sign In   Alert Leve

COMPANY   SOLUTIONS   INSIGHTS

Home > MS-ISAC > SLCGP

## State and Local Cybersecurity Grant Program (SLCGP)

The State and Local Cybersecurity Grant Program (SLCGP) has introduced an unprecedented opportunity for governments below the federal level to apply whole-of-state cybersecurity models to meet the persistent cyber threats they face. Information on the grant program, which is administered by the US Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), can be found at **cisa.gov/cybergrants**. FAQs are available at **https://www.cisa.gov/cybergrants-faq** and **https://www.fema.gov/sites/default/files/documents/fema_slcgp-faq_112022.pdf**.

One of the requirements of the grant program is a State Cybersecurity Plan. The MS- and EI-ISAC, the Center for Internet Security (CIS), and CISA are able to support numerous required elements of your State Cybersecurity Plans as follows.

Manage, monitor, and track information systems, applications, and user accounts +

Monitor, audit, and track network traffic and activity to/from information systems, applications, and user accounts +

# SLCGP Road Map -16 Required Elements - A Better Way to Display - SLCGP (cisecurity.org)

Manage, monitor, and track information systems, applications, and user accounts

CIS | MS-ISAC

CISA Offerings

Open Source Offerings

Best Practices

Manage, monitor, and track information systems, applications, and user accounts

CIS | MS-ISAC

No-Cost Offerings

- CIS Controls/Companion Guides
- CIS Benchmarks
- CIS Hardware & Software Asset Tracker

Fee-Based Offerings

- CIS Endpoint Security Services
- CIS CyberMarket (Tanium)

# SLCGP Road Map -16 Required Elements - A Better Way to Display - SLCGP (cisecurity.org)

Manage, monitor, and track information systems, applications, and user accounts

CIS | MS-ISAC

CISA Offerings

Open Source Offerings

Best Practices

Open Source Offerings

Asset Inventory Tools:

- Snipe-IT
- OpenAudIT
- Nmap
- Zenmap

Identity Access Mgmt & MFA Tools:

- Authentik
- Ory
- PrivacyIDEA

# FY2022 Cybersecurity Plan Projects

## EDR / MDR

- Procure/Distribute Advanced Endpoint Security
- *Required Elements 1,2,12*

## Cyber Assessments

- Utilizing Mi-Deal Contracts to provide Cybersecurity Assessments
- *Required Elements 1,2,3,4,5,6,9,10,14*

## Incident Response

- Provide IR Planning assistance and IR training
- *Required Elements 1,3,5,7,8,9,10,14*

*March 2024*

*June 2024*

*September 2024*

# FY2023 SLCGP

## Application

- Submitted and Approved by CISA & FEMA

## Funding

- $9.6M FY23 Funds on hold pending approval of projects

## Plan Projects

- Sub-Granting Projects | New Project Requests
- Committee working on projects to submit

December 2023

September 2024

December 2024

# Appropriate Use of SLCGP Funds

## What can funds be used for & Who approves these funds

### Acceptable use of Funding

Funds must be used for projects that align with the State & Local Cybersecurity Grant program goals and objectives

1. Cybersecurity Assessments
2. Purchase of MFA Tokens / Keys
3. Endpoint detection and Response Subscriptions/Licensing
4. Network Monitoring Solutions
5. Services to Migrate to the .GOV Domain
6. Dedicated funding to provide training for our cybersecurity professionals
7. Costs for cybersecurity services provided by Managed Service Providers

Just a few examples that align with the cybersecurity plan, and grant objectives.

### The Cybersecurity Planning Committee

Determines what projects will be funded by the State & Local Cybersecurity Grant Program

1. Responsible for ensuring that projects align with the cybersecurity plan and grant objectives.
2. Determine if projects meet one or more of the 16 required elements of the cybersecurity plan.
3. Determine if projects fall under one of the four grant objectives

# What is Supplanting & Why Does it Matter?

| | |
|---|---|
| **Supplanting** | If something is already appropriated in the budget at the State or Local level for the same item(s) the grant funds will be covering, the grant funds **cannot** be used to replace those appropriated dollars. |
| | If you are increasing what's already been appropriated at the State or Local level, you can use grant funds. i.e., expanding, enhancing; anything "on top of" is okay, but it cannot be replaced. |
| | Two key words with supplanting are appropriated and replaced. |
| | Enhancing/upgrading an existing system is supplementing, not *supplanting.* |
| | Going from a "light" version of a product to a more robust version is *not* considered supplanting – it is more of an upgrade. |

Supplementing is allowable for this grant. ***Supplanting* is NOT.**

# Resource Links & Information

## State of Michigan

- Michigan SLCGP Website : DTMB - State and Local Cybersecurity Grant Program (SLCGP) (michigan.gov)
- Michigan SLCGP Participation Survey : https://dtmb.state.mi.us/DTMB_MCSSurvey Password : 2022state038grant
- Local Consent Agreement for FY2022 Grant Funds - State of Michigan FY2022 SLCGP Local Consent Agreement
- SLCGP New Project Request - SLCGP FY2023 + New Project Request Application
- Email questions or general grant information – DTMB-CIP-SLCGP@michigan.gov
- Michigan Secure App - DTMB - Michigan Secure - Slide Included

## CISA | MS-ISAC | FEMA Resource(s) Links

- CISA Cybergrants Website: https://www.cisa.gov/cybergrants-faq
- SLCGP Road Map – Partner supporting required elements offerings : SLCGP (cisecurity.org)
- SLCGP FY2023 NOFO - The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2023 State and Local Cybersecurity Grant Program | FEMA.gov
- SLCGP CISA Website : State and Local Cybersecurity Grant Program | CISA
- FEMA SLCGP Website: State and Local Cybersecurity Grant Program | FEMA.gov

# Michigan Secure

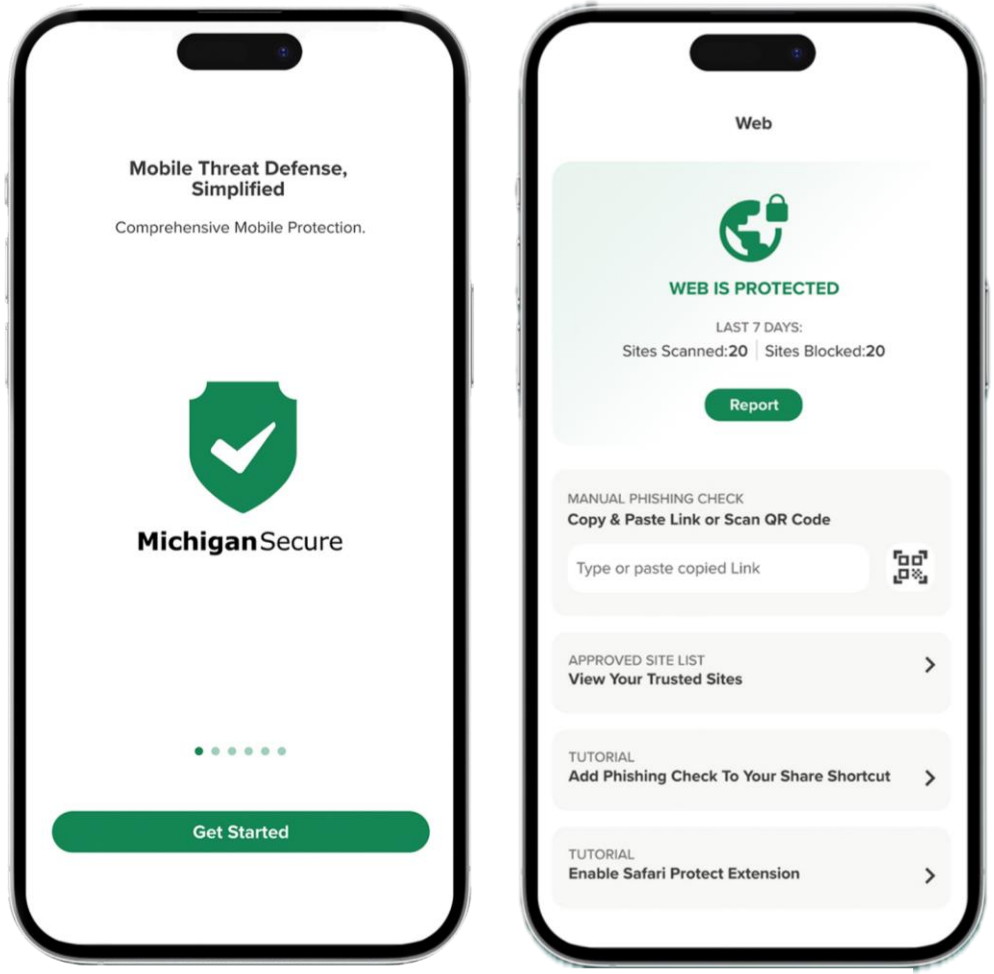
**Michigan Secure** is a free mobile protection app for Michigan residents.

**Michigan Secure** has many features, including:

- App risk lookup and privacy summary
- Phishing protection
- Risky QR code detection
- Threat zone detection
- Unsecure Wi-Fi alerts

No user data is collected.

Learn more at Michigan.gov/MichiganSecureApp.




Download on the App Store

GET IT ON Google Play


# Questions
# ??


# Questions & Updated Information:

**State Local Cybersecurity Grant Program**

www.michigan.gov/cybergrants

dtmb-cip-slcgp@michigan.gov

**SLCGP Interest Survey**

https://dtmb.state.mi.us/DTMB_MCSSurvey
Passcode : 2022state038grant

**Michelle McClish**

External Engagements Lead | Michigan Cyber Security
Cybersecurity & Infrastructure Protection
State of Michigan – DTMB
McClishM@michigan.gov | 517-599-6643