GOVERNOR'S CYBERSECURITY SUMMIT 2023

# STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

WISCONSIN DEPARTMENT OF ADMINISTRATION DOA.WI.GOV

WISCONSIN WEM EMERGENCY MANAGEMENT

# AGENDA

- Introductions
- SLCGP Grant Overview
- Funding to Wisconsin and General Eligibility
- Key Requirements – The Committee and the Cyber Plan
- Implementation
- What Comes Next

# PRESENTERS

- James Sylla, Department of Administration (DOA), Division of Enterprise Technology (DET), Deputy Administrator/CIO
- Katie Sommers, Wisconsin Emergency Management (WEM), Bureau Director for Policy and Grants
- In the audience: Bill Nash (past DET CISO) (William.Nash@cisa.dhs.gov) and Dan Honore (Daniel.Honore@cisa.dhs.gov) both with the Cybersecurity and Infrastructure Security Agency (CISA)
- Who is in attendance today?

# GRANT OVERVIEW

- September 2022: FEMA and CISA release State and Local Cybersecurity Grant Program (SLCGP) Notice of Funding Opportunity (NOFO), the FFY23 NOFO was released August 2023
- In Wisconsin the Department of Administration (DOA) and Wisconsin Emergency Management (WEM) coordinate program delivery
- Federal fiscal years 2022-2025; each has a four-year grant performance period = seven years of activity
- Funding requirements:
  - At least 80% → local units of government
  - At least 25% of all funds → rural communities (jurisdictions with a populations of 50,000 or less)
  - No more than 20% → state agencies

# FUNDING AMOUNTS

| | Federal Funds | % Cost Share | Cost Share Requirement | Total |
|---|---|---|---|---|
| FFY 2022 | $3.7 million | 10% | n/a* | $3.7 million |
| FFY 2023 | $7.6 million | 20% | $1.9 million | $9.5 million |
| FFY 2024 | *$6 million* | *30%* | *$2.6 million* | *$8.6 million* |
| FFY 2025 | *$2 million* | *40%* | *$1.3 million* | *$3.3 million* |

NOTE: Amounts in italics are estimates. Federal Fiscal Years (FFYs) = Oct. 1 of previous year to Sept. 30.

* Wisconsin has received a cost share waiver for FFY2022.

Wisconsin is unlikely to receive cost share waivers for future grant years.

# ELIGIBILITY

- Eligible subrecipients: tribes, counties, municipalities, K-12 school districts, and publicly-owned utilities
- Local funding options per the NOFO:
  - Direct subgrants to eligible applicants
    - Example: To procure products, licensing, and support services
  - Centralized services provided through state agencies or contractors with written consent from eligible applicants
    - Example: Cybersecurity training

# THE FUNDING CHALLENGES

## Funding Challenges

1. The grant provides for four federal fiscal years of funding. While there is a push for funding beyond the four years there is nothing currently defined.
2. The grant has limited dollars. The needs across Wisconsin are greater than can be met by the funds available through this one program.

## The Approach

Focus on improving fundamental cybersecurity needs while building upon existing platforms that will provide a sustainable longer-term impact.

# KEY REQUIREMENT ONE – A CYBERSECURITY PLANNING COMMITTEE

In Wisconsin the state's Cyber Subcommittee, a component of the state's Homeland Security Council, is the approving authority for all activities of the grant. At least half of the members must have cybersecurity experience. Wisconsin members currently include:

- Trina Zanow, Co-chair (Administration)
- Col. Jeannie Jeanetta, Co-chair (Military Affairs)
- Robert Kehoe (Elections)
- Mary Beth Lewis (WE Energies)
- Ed Murphy (University of Wisconsin)
- Marshall Ogren (Justice)
- Jay Schaefer (Winnebago County)
- Ed Snow (Educational Communications Board)
- Ruhamah Bauman (Military Affairs)
- Jennifer Mueller (Health Services)
- Lucas Munz (Public Instruction)

# KEY REQUIREMENT TWO – THE CYBERSECURITY PLAN

- Must be approved by FEMA and CISA
- Approved by the State Homeland Security Council's Cybersecurity Subcommittee; submitted to FEMA in September and approved
- As part of the plan, the State identified projects that will enhance the State's cybersecurity posture

# PROGRAM OBJECTIVES FROM THE STATE PLAN

| Cybersecurity Program | |
|---|---|
| **Program Goal** | **Program Objectives** |
| **1. Improve K-12, local government, and publicly owned critical infrastructure capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity** | **1.1 Perform risk assessments for local units of government.**<br>**1.2 Provide technical assistance to update local endpoints in line with cybersecurity best practices.**<br>**1.3 Establish baseline and enhanced baseline for local units of government.** |
| **2. Increase K-12, local government , and publicly owned critical infrastructures understanding of cybersecurity best practices.** | **2.1 Enroll local government, K-12, and publicly owned critical infrastructure in MS-ISAC and EI-ISAC.**<br>**2.2 Increase local government, K-12 and publicly owned critical infrastructure usage of baseline and enhanced baseline for endpoints and information systems.** |
| **3. Ensure personnel are appropriately trained in cybersecurity.** | **3.1 Make cybersecurity awareness training available to local units of government.**<br>**3.2 Provide scholarships for local government employees to receive cybersecurity certifications.** |

# CYBERSECURITY PLAN – PROJECTS

- First – Flexibility!!
- Units of government with the greatest need will be prioritized
- Update local endpoints and information systems as described in the NOFO
  - Endpoint Protection
  - MFA
  - Enhanced logging
  - System backups
  - End usage of unsupported/end-of-life software and systems
  - Data encryption

# CYBERSECURITY PLAN – PROJECTS (CONTINUED)

- Cybersecurity training for local government IT professionals
  - Focused on universally-recognized and tiered education based on need and current skills
- Encourage all local units of government to enroll in EI-ISAC and MS-ISAC
  - Information services specifically for government entities
- Encourage all local units of government to conduct cybersecurity awareness training annually

# CYBERSECURITY PLAN – PROJECTS (CONTINUED)

- Encourage all local units of government to baseline and incorporate necessary security and privacy controls and cyber best practices
- Encourage all local units of government to adopt the .gov internet domain (preferably the Wisconsin.gov domain, see DET WI Domain Service Request)
- Again, the Cybersecurity Plan and the work can change. Flexibility is important!!

# IMPLEMENTATION

- Up to 20% state projects, other projects executed at the state level for locals (ex. training, contracts)
- Subgrants to units of government with the most need
  - Open application period – applications in WEM's Egrants system
  - Technical assistance with contractual services provided by DET
- Completion of Nationwide Cybersecurity Review required as grant condition
  - Open annually October-February

# WHAT COMES NEXT?

- Developing application materials and scoring criteria for the grant projects
  - Application period likely spring 2024
  - All applicants required to complete a self-assessment of cybersecurity best practices
  - All subgrantees will be required to enroll in no-cost CISA cyber hygiene services
- New DET Chief Information Security Officer (CISO), Troy Stairwalt, coming onboard in November from Ohio

# WHAT COMES NEXT?

- Finalize statewide training offerings
- Submit detailed projects to FEMA for release of funds
- Establish grant application and award process in WEM's Egrants, grant management system
- Outreach – please invite us to your events, especially Jan.-Feb. 2024!
  - In-person presentations
  - Webinars
  - Websites

# WHO ARE THE CURRENT POINTS OF CONTACT?

- DET
  - Matt Michel (Project Manager) – MatthewA.Michel@wisconsin.gov, 608-267-3827
  - James Sylla (Deputy CIO)- James.Sylla@wisconsin.gov, 608-264-6186
- WEM
  - Katie Sommers (Bureau Director, Policy & Grants), Katie.Sommers@widma.gov, 608-242-3222
  - Marc Couturier (Grant Manager), Marc.Couturier@widma.gov, 608-242-3258
- Contact Email: SLCGP@wisconsin.gov
- Other federal points of contact for Wisconsin - Bill Nash (past DET CISO) (William.Nash@cisa.dhs.gov) and Dan Honore (Daniel.Honore@cisa.dhs.gov) both with the Cybersecurity and Infrastructure Security Agency (CISA)

# OTHER INFORMATION

- The federal NOFO listed key positions – the State CIO, the State CISO, and the State Administrative Agency (SAA) contact that works with FEMA.
- SLCGP grant information for Wisconsin can be found at - https://det.wi.gov/Pages/Cybersecurity_Grants.aspx
- September 27th FEMA and CISA released the Tribal Cybersecurity Grant Program (TCGP) - Tribal Cybersecurity Grant Program | CISA