



# State and Local Cybersecurity Grant Program (SLCGP)

2<sup>nd</sup> Round Funding Application Webinar



# Webinar Agenda

1. SLCGP Overview
2. SLCGP Cycle 2 Funding Opportunity
3. Application Requirements
4. SLCGP Grant Requirements
5. Questions



# SLCGP Overview

- The goal of SLCGP is to assist state, local, and tribal governments with managing and reducing cybersecurity risks and threats.
- Joint effort between FEMA and CISA (Cybersecurity and Infrastructure Security Agency).
- There are four objectives for SLGP funding:
  - 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. **This will be a main focus for FY '23 applications.**
  - Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.



# SLCGP Overview

- Grant funding is available through four distinct federal years of funding:
  - FY 2022, FY 2023, FY 2024, and FY 2025.
  - Each year of funding has a four-year performance period for the state.
  - There is a cost share requirement for the grant. For the FY 2022 and FY 2023 grants, this has been waived.
  - Cost share requirements for FY 2024 and FY 2025 grants are 30% and 40%.
- WEM (SAA) is the recipient of funds but must work in coordination with DET and the Cybersecurity Subcommittee of the Homeland Security Council.
- FY '23 and future SLCGP grant funding is contingent upon WEM receiving federal funds from FEMA.



# SLCGP Overview

- Eligible applicants for the subgrant include local governments (county/municipality), tribes, school districts, public utilities, and any other unit of local government/public entity.
  - Non-profit and private organizations are not eligible.
- Applicants can apply for their jurisdiction or can apply as part of a multi-entity application.
- SLCGP applications can request any amount of funding up to \$100,000 per entity.
  - For multi-entity applications, the cap is determined by the number of entities.



# SLCGP Overview

- Allowable activities under the subgrant include:
  - Multi-Factor Authentication (MFA)
  - Endpoint Detection and Response (EDR)
  - Managed Detection and Response (MDR)
  - Extended Detection and Response (XDR)
- The FY '22 grant allowed for MFA and MDR, the FY '23 grant expands on the allowable activities.
- The FY '22 grant awarded over \$3,000,000 to school districts, counties, cities, villages, towns, and multi-entity groups (e.g., multiple school districts)



# SLCGP Cycle 2 Funding Opportunity

- The Notice of Funding Opportunity (NOFO) is published on our website:
  - <https://wem.wi.gov/available-grants/>
- The NOFO includes pertinent information about the grant process, as well as the terms and conditions from both DMA WEM and DHS FEMA of a possible award.
- SLCGP is a competitive grant. It is possible that not all applicants will receive funding.
- Applications will be scored at the end of the application period and funding allocated based on scoring.
- As a competitive grant, our ability to provide assistance may be limited.
- The application period for the grant is April 1 – May 30, 2025 (11:59 PM).
  - Late applications **CANNOT** be accepted.
  - If you submit your application and realize you made an error, you may request that the application is returned to you. This **MUST** be resubmitted by the deadline. Any unsubmitted applications will not be considered.



# SLCGP Cycle 2 Funding Opportunity

- After the close of the competitive application period, applications will be scored, ranked, and final funding decisions made.
- This process is also dependent on FEMA, so while our goal is to have grant awards by July 1, this process may be delayed due to FEMA responsiveness.
- Notifications of application decisions will be sent via email.
- Even if you receive a notice of award email, **DO NOT BEGIN YOUR PROJECT** until award documents are received.
- You may be selected for a full award or partial award depending on funding available and allowability of projects applied for.





# Application Information

- To access the application: <https://wem.egrants.us>.
  - There is an Egrants User Guide available on the homepage.
  - New Egrants users will click “register here” button to register for an account.
    - **It may take a few business days to process accounts, do not wait until the last day!**
- The NOFO details all sections that will be required to be completed.
- The performance period of the grant is suggested in the NOFO as 7/1/2025-8/31/2027.
- Most sections are simple questions e.g., Is your entity rural? Is this a multi-entity application?



# Application Information

- Competitive applications are scored, so answers to narrative questions describing your evidence of need or the project implementation are very important.
- The application asks for a timeline of the project. This is to ensure that your project timeline is feasible within the parameters of the grant.
- Supporting documentation that assists with your grant application include quotes from vendors (not invoices!) or cybersecurity vulnerability scan results (do NOT send the whole vulnerability scan!).
  - Multi-entity applicants will include information on the other entities for the application in an attached document.



# Application Information

- Applicants must have a Unique Entity Identifier (UEI) through SAM.gov to be eligible for an award.
- Registration in SAM.gov is free.
- There will be two sessions of “Office Hours” hosted via Teams in May for application questions and Egrants assistance.
  - [May 14, 2025, 9-11 am](#)
  - [May 29, 2025, 1-3 pm](#)



# SLCGP Grant Requirements

- SLCGP has federal requirements for the SAA and any subgrantees who receive SLCGP funding.
  - National Cybersecurity Review (NCSR)
    - Grant recipients must complete the Nationwide Cybersecurity Review (NCSR) prior to grant close Year 1 and then annually for each year funding is approved. The NCSR is available each year from October through February at <https://www.cisecurity.org/ms-isac/services/ncsr>.
  - Cyber Hygiene Services
    - Grant recipients must sign up for free cyber hygiene services through CISA: <https://www.cisa.gov/cyber-hygiene-services>.



# SLCGP Grant Requirements

- Semi-annual reporting in Egrants is required (January / July).
- Program Reports
  - There are several questions that are required to track the progress and status of your grant to include activities completed in each reporting period.
- Fiscal Reports
  - Fiscal reports are the mechanism for requesting reimbursement for costs incurred.
  - Upload invoices and proofs of payment, as well as a signed reimbursement request form which is available through Egrants.
- Reimbursements will not occur if all reporting is not up to date.



# Questions?



# Contact Information:

SLCGP Grant Manager

Marc Couturier

[marc.couturier@widma.gov](mailto:marc.couturier@widma.gov)

(608)590-9112