SLCGP – Supporting Information

1 FAQ – FREQUENTLY ASKED QUESTIONS

Who can participate?

- All state and local government entities are eligible to participate in the State and Local Cybersecurity Grant Program (SLCGP).
    1. Counties, cities, villages, towns, local public authorities.
    2. School districts, special districts, intrastate districts.
    3. Councils of government, regional or interstate government entities, or agencies or instrumentalities of a local government.
    4. Indian tribes or authorized tribal organizations.
    5. Rural communities, unincorporated towns or villages, or other public entities.
- Ineligible entities include nonprofit organizations and private corporations.
- Federal law requires states to pass through at least 80% of the total funding to local governments through shared solutions/capabilities or subgrants. Further, at least 25% of Wisconsin’s total funding will benefit rural communities, defined as communities with a population of less than 50,000 residents.

How can my organization apply?

- Wisconsin Emergency Management website: Available Grants | Wisconsin Emergency Management.
- The Notice of Funding Opportunity (NOFO) for SLCGP provides comprehensive information on how to apply: Cycle 2 Funding 2023 (wi.gov).
- Organizations are required to apply through the Egrants online system. For information about registering and using Egrants, please see the Egrants System User Guide.

Which project types are eligible for funding?

- Multifactor authentication (MFA)
- Managed detection and response (MDR)
- Endpoint detection and response (EDR)
- Extended detection and response (XDR)

Is equipment eligible for funding?

- No; however, in the grant application, there is a line for equipment because software can meet the federal definition of equipment if it’s sustained for over one year and over a specific cost threshold.

How long can a grant recipient pay for services using grant funding?

- All services must be received within the period of performance of the grant, which starts when the grant is both awarded and accepted by the recipient and ends August 31, 2027. For subscription services, the contract must end on or before August 31, 2027, or the cost of a longer

subscription must be pro-rated to cover only services received on or before August 31, 2027.
- Services may not be purchased or contracted for prior to the date the grant is awarded and accepted by the recipient. No costs incurred prior to this date are eligible for reimbursement.

If we expand our current MFA to more users would this classify as new?

- The grant cannot cover any activities that are already funded or for which funding is planned. Additional licenses can be covered; however, only the costs of the additional licenses can be paid with grant funding.

How long are funds available?

- The program is funded for four federal fiscal years: 2022-2025. Each year of funding has a three-year period of performance.

What are the goals of the SLCGP?

- From the Wisconsin December 2024 Wisconsin Cybersecurity Plan:
  1. Improve K-12 and postsecondary education, local units of government, tribes and publicly owned critical infrastructure capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity.
  2. Increase K-12 and postsecondary education, local units of government, tribes and publicly owned critical infrastructure understanding of cybersecurity best practices.
  3. Ensure personnel are appropriately trained in cybersecurity.

What are the benefits of participating in the SLCGP?

- Participation will enable you to:
  1. Mature cybersecurity capabilities.
  2. Reduce risk by leveraging statewide programs.
  3. Collaborate and share information across entities.
  4. Plan and prepare for cyber incidents.
  5. Keep Wisconsin's data secure.

How can my organization understand our current cybersecurity gaps and capabilities?

- The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, self-assessment offered to all states, local governments, Tribal Nations, and territorial governments through the Center for Internet Security (CIS). This is an excellent way to learn about your organizational baseline. The assessment is open from Oct. 1 – Feb. 28 each year.
- The Cybersecurity and Infrastructure Security Agency (CISA) provides risk and vulnerability assessments as well as other tools for state, local, tribal, and territorial governments. To schedule a Risk and Vulnerability Assessment, contact central@cisa.dhs.gov.

Link to CISA's SLCGP FAQ:
State and Local Cybersecurity Grant Program Frequently Asked Questions | CISA

2 GLOSSARY

2.1 Terms

Term	Definition
Project Director	The individual who is responsible for execution, oversight, and administration of this grant.
Financial Officer	The individual who is responsible and accountable for the financial management of the awarded agency with the authority to certify expenditures for this grant.
Signing Official	The individual who has the authority to sign for and obligate the awarded agency into a legal grant agreement.
Alternate Contact	The individual who is the backup contact in the event the Project Director or Financial Officer is not available. This individual cannot sign or certify on behalf of the Financial Officer or Project Director.
Shared responsibility model	Shared responsibility model describes a model where security and compliance are shared responsibilities between the provider and the customer.

2.2 Acronyms

Acronym	Definition
CISA	CISA stands for Cybersecurity and Infrastructure Security Agency. CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. It falls under the federal Department of Homeland Security and serves as the federal program lead for the SLCGP.
DET	Division of Enterprise Technology (division within DOA)
DMA	Wisconsin Department of Military Affairs
DOA	Wisconsin Department of Administration
EDR	Endpoint detection and response is a cybersecurity solution that continuously monitors endpoint devices to detect and respond to cyber threats.
FEMA	FEMA stands for Federal Emergency Management Agency. FEMA coordinates within the federal government to make sure the nation is equipped to prepare for and respond to disasters. It falls under the federal Department of Homeland Security and serves as the federal grants lead for the SLCGP.
MDR	Managed detection and response provides customers with remotely delivered, human-led turnkey security operations center functions by delivering threat disruption and containment.
MFA	Multi-factor authentication is a workforce service that requires users to provide two or more credentials to verify their identity. MFA adds an extra layer of security by providing strong authentication for your applications.

MS-ISAC	MS-ISAC stands for Multi-State Information Sharing and Analysis Center. It is a CISA-supported collaboration with the Center for Internet Security designed to serve as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.
SLCGP	State of Local Cybersecurity Grant Program
WEM	Wisconsin Emergency Management (division within DMA)
XDR	Extended detection and response is a cybersecurity approach that unifies threat data from various security tools across an organization enabling faster and more accurate threat detection.

3 CYBERSECURITY RESOURCES

- Cybersecurity Infrastructure & Security Agency (CISA)
    - State and Local Cybersecurity Grant Program | CISA
    - State and Local Cybersecurity Grant Program Frequently Asked Questions | CISA
    - FFY23 State and Local Cybersecurity Grant Program Fact Sheet | CISA
    - Free Cybersecurity Services and Tools | CISA
    - Cybersecurity Training & Exercises | CISA

- Wisconsin Emergency Management (WEM)
    - Available Grants
    - Egrants System User Guide
    - Wisconsin Cyber Response Team

- Division of Enterprise Technology (DET)
    - Cybersecurity
    - Cybersecurity Grants

4 CONTACT

SLCGP Mailbox - SLCGP@wi.gov