SLCGP – Supporting Information

1. FAQ

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. Authorized Tribal governments and organizations.
    5. Rural communities, unincorporated towns or villages, or other public entities.
        - ✓ (see https://www.cisa.gov/cybergrants/slcgp for more information)

How can my organization participate?

- Expect an update to this document by May 15, 2024, with more details.

What are the goals of the SLCGP?

- From the Wisconsin August 2023 Wisconsin Cybersecurity Plan:
    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.
    2. Increase K-12, local government, and publicly owned critical infrastructure understanding of cybersecurity methods.
    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 (and agencies), local governments (and departments), 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 October 1 - February 28 each year. If selected for SLCGP funding, your organization will be required to complete this assessment for every year of your grant. Your organization can review NCSR information and register at Nationwide Cybersecurity Review (NCSR).

Funding timeline and process

How is the SLCGP funded?

- Over the next four years (July 1, 2023 - June 30, 2027), the Whole-of-State Cybersecurity Plan will include $19.3 million of federal SLCGP funds.

- This grant program is not expected to be renewed by the federal government at the end of the four years. The required matching fund percentage increases each year to encourage state and local governments to develop sustainable funding for efforts that will last longer than the four-year SLCGP.

Federal Fiscal Year	Federal Funds	% Cost Share	Cost Share Requirement	Total
2022	$3.7 million	10%	n/a*	$3.7 million
2023	$7.6 million	20%	$1.9 million	$9.5 million
2024	*$6 million*	*30%*	*$2.6 million*	*$8.6 million*
2025	*$2 million*	*40%*	*$1.3 million*	*$3.3 million*
Italic indicates an estimate. The Federal Fiscal Year runs Oct. 1 of prior year to Sept. 30. Wisconsin has received a cost share waiver for FFY2022.				

What has been done so far?

- Wisconsin completed the first steps to access the federal money – creating a planning committee (Wisconsin Cybersecurity Subcommittee) and completing a cybersecurity plan that was approved by FEMA and CISA (State of Wisconsin Cybersecurity Plan).
- With the launch of the State of Wisconsin Cybersecurity Plan, Wisconsin is taking the next step to inform and engage local government entities who are eligible for SLCGP grant funding.

When will the federal funds be available in Wisconsin?

- Federal funds for SLCGP programs will be released in response to specific project requests that Wisconsin makes to the federal government. These project requests must follow an application and selection cycle with eligible local governments.
- The Wisconsin Cybersecurity Subcommittee will only submit project requests that align with the Cybersecurity Plan. The plan is to allow

one application period for each grant funding year. If there are not enough eligible projects to fully use the funding, additional application periods may be opened.

How much of this federal funding will benefit local governments?

- Wisconsin is committed to ensuring the funding from this grant program supports as many local government organizations as possible. Federal law requires states to pass through at least 80% of the total funding to local governments through shared solutions/capabilities or a sub-grant process. 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 long will it take to get access to funding or programs?

- The federal grant requires Wisconsin to pass through local funding no later than 45 days after FEMA releases the funding to the state. Based on this requirement, Wisconsin will submit one request for release of funding after each application period and award the funds for the selected projects no later than 45 days after receiving the funding from FEMA.

Here is a link to the CISA SLCGP FAQ:
State and Local Cybersecurity Grant Program Frequently Asked Questions | CISA

2 GLOSSARY

2.1 Terms

Term	Definition
Project Director	For this grant, select the individual who is responsible for execution, oversight, and administration of this grant.
Financial Officer	For this grant, select the individual who is responsible and accountable for the financial management of the awarded agency with the authority to certify expenditures.
Signing Official	For this grant, select the individual that has the authority to sign the legal agreement and obligate your agency into a legal grant agreement.
Alternate Contact	This individual 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 (within DOA)
DMA	Department of Military Affairs
DOA	Department of Administration
ESS	Endpoint Security Services: Endpoint security, also known as endpoint protection, is a set of technologies and practices that protect devices used by end users from unwanted, malicious software.
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.
IaaS	IaaS stands for Infrastructure as a Service. It provides the infrastructure for running applications or other processes in the cloud.
MDR	Managed detection and response (MDR) services provide customers with remotely delivered, human-led turnkey security operations center functions by delivering threat disruption and containment.
MFA	Multi-factor authentication (MFA) 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 cloud, web-based, on-premises, SaaS, and IaaS 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, territorial, and tribal governments.
PaaS	PaaS stands for Platform as a Service. It is a complete cloud environment that includes everything developers need to build, run, and manage applications—from servers and operating systems to all the networking, storage, middleware, tools, and more.
SaaS	SaaS stands for Software as a Service. It provides access to applications hosted in the cloud. An example would be an application used to pay for local parking spots.
SLCGP	State of Local Cybersecurity Grant Program https://www.cisa.gov/state-and-local-cybersecurity-grant-program.
WEM	Wisconsin Emergency Management (division within DMA)

3 TIPS

- **Use of Grant Funds** - Grant funds may not be used for construction, renovation, remodeling, or performing any type of physical alterations to buildings or other facilities. This can be as minimal as drilling a new hole in a wall to run a cable.

4 CYBERSECURITY RESOURCES

- Cybersecurity Infrastructure & Security Agency (CISA)
  - State and Local Cybersecurity Grant Program | CISA
  - State and Local Cybersecurity Grant Program Frequently Asked Questions | CISA
  - FY22 State and Local Cybersecurity Grant Program Fact Sheet | CISA
  - Free Cybersecurity Services and Tools | CISA
  - FedVTE Public Courses Page (usalearning.gov)
  - Cybersecurity Training & Exercises | CISA

- Wisconsin Emergency Management (WEM)
  - Available Grants
  - Wisconsin Cyber Response Team

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

5 CONTACT

- SLCGP Mailbox - SLCGP@wi.gov