SLCGP – Supporting Information

1. FAQ – FREQUENTLY ASKED QUESTIONS 2

2 GLOSSARY 8

2.1 Terms 8

2.2 Acronyms 8

3 TIPS 9

4 CYBERSECURITY RESOURCES 9

5 CONTACT 10

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. 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 apply?

- Wisconsin Emergency Management home site: 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)
- If your organization has questions about how to setup a login for Egrants, please see the Egrants System User Guide.
- Egrants login.

How long can a grant recipient pay for services if they are billed up front?

- FFY 2022- 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, 2026. For subscription services, the contract must end on or before August 31, 2026, or the cost of a longer subscription must be pro-rated to cover only services received on or before August 31, 2026.

- FFY 2023- 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.

How is the SLCGP grant different from other federal grants delivered through the grants.gov portal?

- This grant is a passthrough grant meaning the funds pass through the state before being awarded to local communities, school districts, etc. The state (Wisconsin Emergency Management) applies to the federal government and the local communities, school districts, etc. apply to the state using the state's Egrants system.
- Some other federal funding opportunities allow local communities, school districts, etc. to apply directly to the federal government for funding, but not SLCGP.

May the funding be used to contract and pay up front for 3 years of services?

- FFY 2022 - The funds can be used for activities that go up to the end of the performance period of the grant, but it is important they have a plan for after the funding expires. The period of performance for the first funding cycle ends August 31, 2026.

- FFY2023 - The funds can be used for activities that go up to the end of the performance period of the grant, but it is important they have a plan for after the funding expires. The period of performance for FFY 2023 funding cycle is July 1, 2025, and ends on August 31, 2027.

Are multiple year licensing agreements allowed under the grant for Multifactor Authentication (MFA) and Managed End Point Detection and Response (MDR) solutions?

- Only the time frame for the license expense that is covered by the period of performance for a subgrant is eligible for reimbursement of costs from a grant. It depends on how long the period of performance of their subgrant ends up being on their application and the time of award/approvals.

- With the applications for May 30th cycle - there's time for applicants to request a subgrant that's close to two years (July 1, 2025 – August 31, 2027).

May the funding be used to cover additional hardware to read YubiKeys?

- Purchasing new laptops is not eligible. External YubiKey NFC readers may be eligible.

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

- Additional licenses can be covered, as well as adding licenses to a system that doesn't have it; however, it is only the costs of the additional licenses that would be covered with grant funding. To clarify, only the expansion of what is already in place would be classified as new and could be covered under the grant. If they expand it does not mean all the MFA/MDR can be covered, just the expanded portion.

How long are funds available?

- Funds are available for four fiscal years, and the funding can extend to seven years. However, receiving an award in one year does not guarantee receiving an award in subsequent years.

Can entities apply for funds to offset existing EDR costs?

- No, costs for existing solutions are not eligible for reimbursement.

If we have an EDR solution, can we apply for funds to implement XDR in tandem?

- A grant application needs to be submitted and approved for a new project to implement XDR. Costs are not eligible for any work done prior to the grant award.

Would round 1 grant recipients be able to apply for round two to extend the implementation of their round 1 solution?

- A recipient of Cycle 1 funding who would like to apply for Cycle 2 to cover what Cycle 1 has covered is eligible if the period of performance for the next grant starts after their current grant ends. (i.e. ABC County has a grant that covers MFA & MDR that goes through June 30, 2026, they could apply for Cycle 2 funding that covers the exact same project if it starts July 1, 2026.)

- If you are funding your current EDR/MFA through SLCGP Funds and would like to apply for additional funding through Cycle 2 reach out to Marc.couturier@widma.gov for questions specific to your specific situation.

Note: Grant funding cannot be used to fund existing solutions that are funded through the applicant's own budget or another grant's funding

What are the goals of the SLCGP?

- From the Wisconsin December 2024 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?

- The SLCGP is 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 Funds	% Cost Share	Cost Share Requirement	Total
FFY 2022	$3,795,634	10%	n/a*	$3,795,634
FFY 2023	$7,666,939	20%	n/a*	$7,666,939
FFY 2024	$ 5,890,643	30%	$2,524,562	$8,415,205
FFY 2025	*$2 million*	*40%*	*$1.3 million*	*$3.3 million*

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

* Wisconsin has received a cost share waiver for FFY 2022 and FFY 2023.

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

What has been done so far?

- Wisconsin completed the first steps to access the federal money – creating a planning committee (Wisconsin Cybersecurity Subcommittee updated in the Cybersecurity Plan) 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.

Can a consortium participate in the SLCGP program?

- The consortium can assist a member in applying on their own behalf or on behalf of multiple members, but only units of government (local, state, tribal) can be applicants.

May pre-implementation assessments / audits needed to scope an MFA or MDF project be eligible for funding?

- An assessment or audit necessary to plan/scope out an MFA or MDR project would not be eligible activities for the first year's funds. It is expected that the applicant will know the scope of their project when making the request.
- FYI, CISA provides free cybersecurity assessment services if needed. Free Cybersecurity Services & Tools | CISA

Link to CISA's SLCGP FAQ:

- State and Local Cybersecurity Grant Program | CISA
- FFY 2023 State and Local Cybersecurity Grant Program FAQs

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 the 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 the 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
  - 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

5 CONTACT

- SLCGP Mailbox - SLCGP@wi.gov