



Wisconsin State and Local Cybersecurity Grant Program

▶ FY '24 ROUND 3



Cyber incidents are growing amongst municipalities

AND WISCONSIN IS NO EXCEPTION

Washburn County

August 2026

All county technology shut down. Phones and email went down, and residents were told to call 911 to reach any department.

Iowa County

April 2025 — still recovering

Ransomware deleted a significant portion of the network including backups. Land records restoration is contracted into 2026.



Rusk County

March 2026

The county reported a cybersecurity incident. The Qilin ransomware group later claimed responsibility on its leak site.

WI water utilities

July–August 2026

DNR issued a statewide alert over activity targeting utility control systems. FBI and EPA warned of utilities affected in seven states.

Why municipalities are targeted

IT IS NOT ABOUT SIZE



Low tolerance for downtime

Permitting, courts, utility billing, payroll and dispatch all must keep running. That pressure is what extortion relies on.



Valuable records

Property and land records, police records, vital records and resident data all carry value on the open market.



Constrained resources

Small IT teams and aging infrastructure, with cybersecurity competing against direct service delivery for budget.

Smaller communities are targeted more, not less.

Wisconsin FY24 SLCGP at a glance

THE BASICS YOU NEED TO KNOW

THE FUNDING

- Wisconsin is releasing \$4,712,514.40
- Up to \$100,000 maximum award per entity
- 100 anticipated awards
- No cost share — the 30% match is waived for this cycle

WHO CAN APPLY

- Counties, municipalities, towns and villages
- School districts, special districts, public utilities
- Councils of government, tribal governments
- Non-profit and private organizations are not eligible

KEY DATES

- Applications opened August 17, 2026
- Application due October 30, 2026
- Anticipated notice of award February 15, 2027
- Grant performance period March 1, 2027 – August 31, 2028 (18 months)

This is the last round with no cost share

Per Wisconsin Emergency Management, this is the third of four cycles of funding and the last cycle with no cost share requirement. Future cycles of this grant will carry a 40% cost share.

IMPORTANT ITEMS TO NOTE

- No supplanting — grant funds cannot replace money already in your budget
- No duplication of benefits with other awards for the same purpose
- No pre-award costs — nothing before a signed agreement is reimbursable

Cybersecurity tools that qualify for funding

STRAIGHT FROM THE NOTICE OF FUNDING OPPORTUNITY

Multi-Factor Authentication (MFA)



Requires two or more credentials to verify a user's identity, adding a layer of protection for applications and accounts.

Managed Detection and Response (MDR)



Continuous monitoring of endpoints, networks and cloud environments, with investigation and response to identified threats.

Endpoint Detection and Response (EDR)



Continuously monitors endpoint devices to detect and respond to threats.

Extended Detection and Response (XDR)



Unifies threat data from multiple security tools across the organization for faster, more accurate detection.

Security Awareness Training



Helps staff recognize and avoid common attacks. Includes phishing simulations, a training library and reporting.

Internet Edge Security



Next-generation firewall, secure web gateway, DNS and email security, and DDoS protection at the internet edge.

And more...

ALSO ELIGIBLE UNDER THIS ROUND

Migration to the .gov Domain



Vendor support for .gov registration, email migration, and implementation of MFA, MDR, EDR and XDR alongside the move.

Vulnerability Management



Automated scanning that detects known vulnerabilities. The service must scan, assess, remediate or mitigate, then rescan to verify the fix.

Immutable Backups to the Cloud



Backups stored so they cannot be modified, deleted or overwritten for a defined length of time.

Penetration Testing



Identifies vulnerabilities across the environment using both technical tools and social engineering.

For smaller entities, the NOFO recommends starting with training, CISA guidelines, MFA, and a .gov domain.

There are many organizations here to help

AND THEY ARE ALL HERE FOR YOU



Wisconsin Emergency Management & Division of Enterprise Technology

Fund and administer the State and Local
Cybersecurity Grant Program



CISA

Free cyber hygiene services, including
vulnerability scanning, at no cost to your
municipality



League of Wisconsin Municipalities

Coordinates a joint application on behalf of
member municipalities



VC3

Provides technical, vendor-neutral details for
your application, and is one of many providers
that can deliver eligible services

Free CISA cyber hygiene services: cisa.gov/cyber-hygiene-services — the NOFO strongly encourages smaller entities to start here.

Three ways to apply

PICK THE PATH THAT FITS YOUR MUNICIPALITY

1 Work with VC3

You want technical help scoping your project, and you want to be part of the League's group submission.

- VC3 helps you with discovery and understanding what your environment needs.
- VC3 provides a vendor-neutral quote using NOFO terminology.
- VC3 passes your information to the League for the group submission.
- VC3 does not write the grant application.

GET YOUR INFORMATION TO VC3 BY

October 26

2 Go directly through the League

You are not working with VC3, but you still want the benefit of the League's group submission.

- Send your project and cost information straight to the League.
- The League will ask you to complete a short self-certification.
- It confirms you are not supplanting budgeted dollars and that you meet the eligibility rules.
- Later questions can be handled case by case.

GET YOUR INFORMATION TO THE LEAGUE BY

October 2

3 Apply on your own

You would rather file your own application directly with the state.

- Register for access and submit through Egrants at wem.egrants.us.
- You need a valid Unique Entity Identifier (UEI) in SAM.gov first.
- You own the narrative, the budget detail and the attachments.
- Submit questions to SLCGP@wi.gov.

SUBMIT TO THE STATE BY

October 30

However you apply, two things stay the same.

The League is the grant recipient and sub-grants to participating members, so approved expenses are reimbursed through them. And federal rules require your municipality to run its own competitive process before selecting a provider. VC3 can assist technically and supply a vendor-neutral quote but cannot write your application or define your procurement.

The fine print

FOUR THINGS THAT SURPRISE PEOPLE

01 It is competitive

- Not all applicants will receive funding.
- Applications are screened for responsiveness, then scored at the end of the period.
- You may be selected for a full or partial award.

02 The deadline is hard

- August 17 – October 30, 2026. Late applications CANNOT be accepted.
- Submitted in error? You can request it back, but it must be resubmitted by the deadline.
- Unsubmitted applications will not be considered.

03 Do not start early

- Awards are targeted for February 15, 2027, but the process depends on FEMA and may slip.
- Even after a notice of award email, do not begin your project until award documents arrive.
- No pre-award costs are reimbursable.

04 You pay first

- Payment is on a reimbursement basis.
- WEM needs at least 30 days to review, and disbursement may take another month.
- Semi-annual Egrants reporting is required, or reimbursements stop.

And one more. Sustainment after the grant period is your responsibility — the application asks for your plan to keep these services running once the funding ends.

Next steps

THE GOAL IS TO KEEP YOU SAFE AND SECURE

1

Decide your path

Direct application through Egrants, or the joint application through the League.

2

Check your UEI

Confirm a valid Unique Entity Identifier in SAM.gov. If you do not have one, start now — this has lead time.

3

Scope your project

Decide which eligible services you want funded, and how many staff and devices they need to cover.

4

Get grant-ready quotes

Implementation and licensing as separate line items, with subscriptions prorated to the 18-month period.

5

Submit before the deadline

October 30, 2026. If you are applying through the League the deadline is October 2, and if you're applying with VC3's help the deadline is October 26.

QUESTIONS?

VC3

Christina Drews

Christina.Drews@VC3.com

League of Wisconsin Municipalities

Zach Vruwink

zvruwink@lwm-info.org

Wisconsin Emergency Management

SLCGP@wi.gov

Additional resources

Notice of Funding Opportunity (NOFO)

[wem.wi.gov — SLCGP Cycle 3 Funding FY2024](#)

Egrants application portal

<https://wem.egrants.us>

WEM SLCGP program page

wem.wi.gov/state-and-local-cybersecurity-grant-program-fy-24-cycle-3-funding-opportunity/

Division of Enterprise Technology

det.wi.gov/Pages/Cybersecurity_Grants.aspx

FEMA program page

fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

Free CISA cyber hygiene services

cisa.gov/cyber-hygiene-services

SAM.gov (Unique Entity Identifier)

sam.gov

Questions to the state

SLCGP@wi.gov



Questions?