State of Maine
State and Local Cybersecurity Grant Program (SLCGP)

Building a Secure Future

Maine's Cybersecurity Initiatives under the SLCGP

November 10, 2026
Presented by Charles X. Rote and Jeremy Cotnoir

Presenters

Charles X. Rote

Chief Information Security Officer
State of Maine

Jeremy Cotnoir

Director of Infrastructure & Cyber Security
Department Of The Secretary Of State

Agenda

- Situation | Cybersecurity Landscape
- SLCGP Overview
- Current Capabilities
- Upcoming
- Stakeholders
- Vendors
- Conclusion



Cybersecurity Landscape

TARGETING

INFRASTRUCTURE ATTACKS

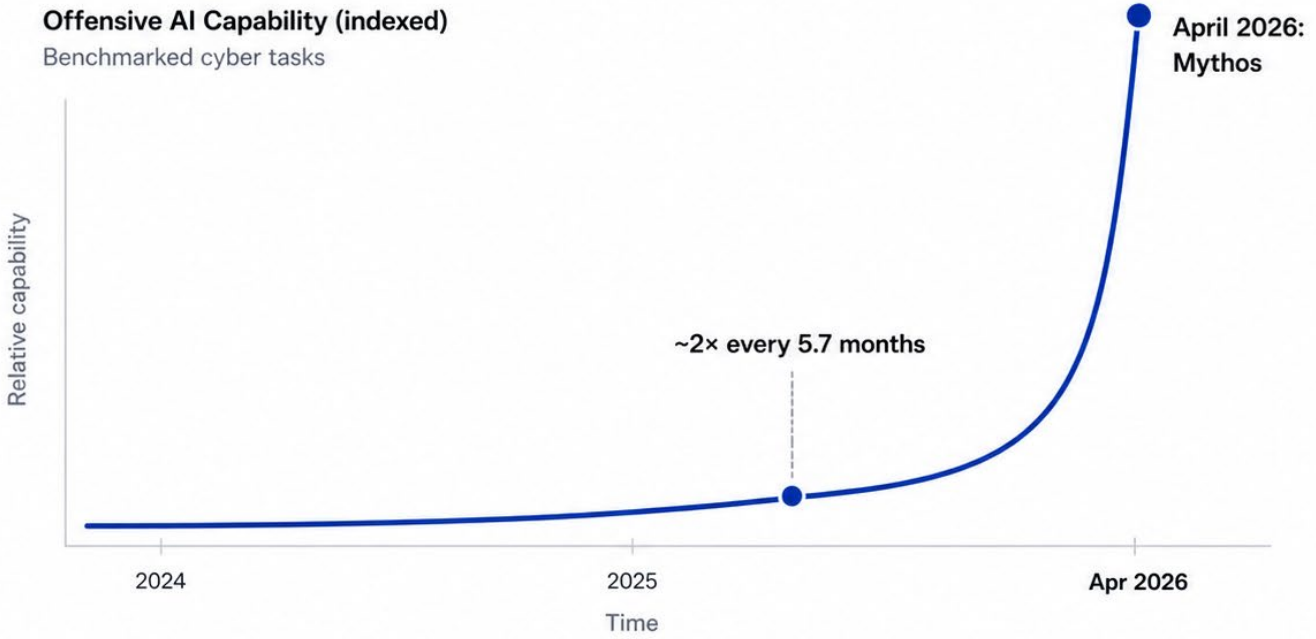
RESOURCE CONSTRAINTS

DATA BREACH PROTECTIONS



What Mythos Found

April 2026 changed the vulnerability landscape



Key Findings

Thousands of zero-days discovered autonomously

27-year and 16-year dormant vulnerabilities exposed

<$50 per vulnerability discovery

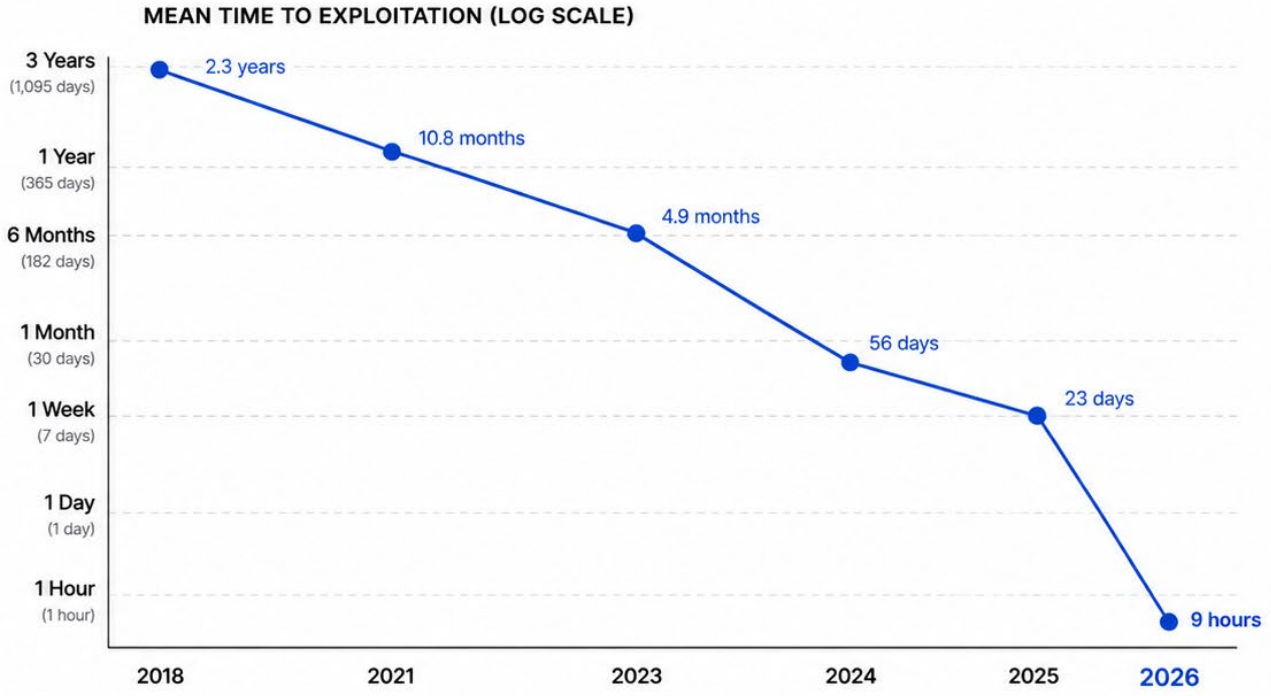
AI is discovering vulnerabilities faster than organizations can inventory them.

AI phishing: **54%** vs **12%** click-through

Source: Anthropic (Apr 7, 2026), Reuters (Apr 8, 2026), Lyptus Research (Apr 2026), Microsoft Security Blog (Apr 2, 2026)

Zero Day Clock: Mean Time to Exploitation

Attackers weaponize vulnerabilities exponentially faster than public disclosure.



KEY TAKEAWAY

~2,200×
faster exploitation
since 2018

MILESTONES CROSSED

- **Under 1 Year** ~2021
- **Under 1 Month** ~2025
- **Under 1 Week** 2026
- **Under 1 Day** 2026
- **Under 1 Hour** ~2026 (projected)
- **Under 1 Minute** ~2028 (projected)

INSIGHT

This is not linear decline—it's exponential collapse.

Process-based defense windows are gone.

Source: Zero Day Clock (Sergej Epp / Sysdig) based on 3,533 CVE-exploit pairs (CISA KEV, VulnCheck KEV, XDB)
Cited in CSA/SANS/OWASP Mythos-Ready Security Program (April 2026)
Authors: Former CISA Director, Former National Cyber Director, Google VP Security Engineering, Bruce Schneier

Cyber Attacks On Infrastructure Are Hitting Home

2021: Maine had its first known ransomware attacks on wastewater plants, in Limestone and Mount Desert. Treatment kept running, but office systems were down for days.

2025: Cybersecurity incidents impacted Covenant Health locations. Connectivity and some business operations were disrupted. More than 284k patients in Maine were affected by the data breach.

2026: Town of Lincoln was hit with a cyber attack that caused closures of municipal buildings. Impacts included several town computer systems, including the main file server and other network infrastructure.

2026: In July, a cyberattack on a telecom company knocked out internet service for 23 midcoast towns, including town office services.



One attack on a shared system can affect many communities and organizations at once.

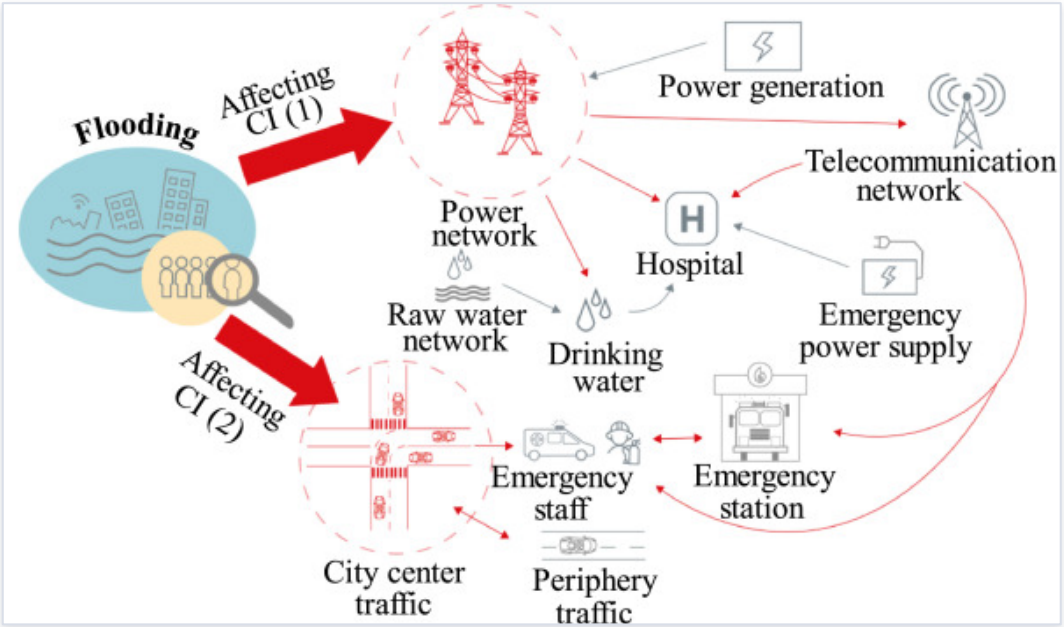
Critical Infrastructure Sectors Depend On Each Other

The critical infrastructure sectors depend on each other, so one disruption rarely stays in one place.

If power goes down, water pumps, hospitals and communications go down with it.

If a network goes down, town offices, 911 dispatch and emergency response slow down.





Impact for Critical Infrastructure

Consequences: What could happen?

- Disruption of Essential Services (the *critical* in critical infrastructure)
- Economic Damages/Impacts
- Public Safety considerations
- Loss of Trust (in government)

So, What Do we Do About It?

- Preparedness: Planning, Training, and Exercise Activities
- Protection and Prevention measures
- Build Resiliency and Have Contingency Measures in Place (Continuity/Disaster Recovery)

The SLCGP in Maine at a Glance

WHAT IT IS

A four-year federal grant (FY22–FY25) to strengthen state and local government cybersecurity. The local cost share rises to 40% in FY25.

WHO GUIDES IT

MEMA and MaineIT, advised by a Planning Committee representing state, county and local government, education, public health, public safety, elections, critical infrastructure and the National Guard.

HOW MAINE USES IT

A FEMA- and CISA-approved Cybersecurity Plan (2024; update coming 2026) makes the State a shared service provider, so towns get vetted tools and training **at no cost to participants**.

Administered by the U.S. Department of Homeland Security (DHS)

Funded by the Infrastructure Investment and Jobs Act (IIJA)

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

Maine SLCGP Funding by Grant Year

Grant Year	Period of Performance	Grant Amount	Match	Participants
FY2022	9/2022 – 11/2026	$2,666,577	10%	99
FY2023	12/2023 – 11/2028	$5,440,000	0%	169
FY2024	2/2025 – 1/2029	$4,070,000	0%	TBD
FY2025	9/2025 – 2/2030	$2,222,299	40%	TBD
Total		$14,398,876 Federal Funds	$1,155,578 State Funds	*190 Unique Entities

Total Cyber Security Dedicated Funds: $15,554,454

*Participant total covers FY2022 and FY2023 unique organizations. Some entities from FY22 reapplied in FY23. FY2024 and FY2025 participants to be determined.

Maine Cybersecurity Plan

Published 2024, Update Coming 2026

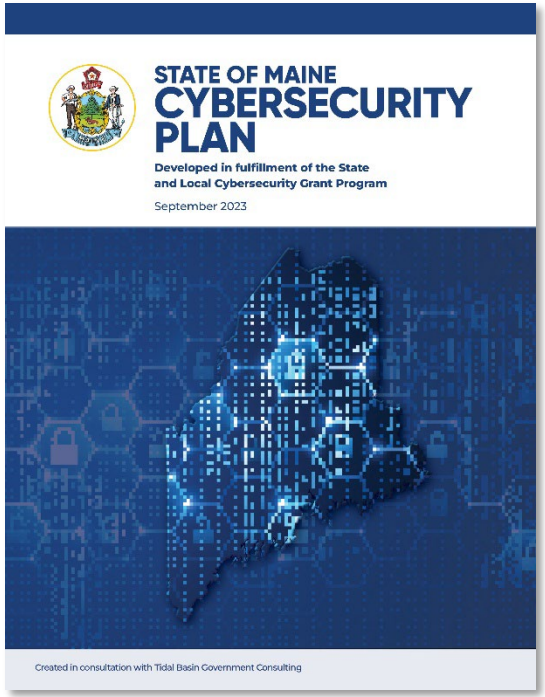
VISION

A cyber-resilient Maine that realizes the opportunities afforded by technological innovation and balances the cybersecurity protections necessary to safeguard its data and critical infrastructure.

MISSION

The State of Maine will lead and coordinate initiatives to reduce cybersecurity risks against State and local government-owned or operated information systems, mitigating the impacts on Maine's essential services and community members.

State of Maine
Cybersecurity Plan



The State of Maine has developed a Cybersecurity Plan (approved by FEMA and CISA) to serve as Maine's strategic roadmap to guide SLCGP implementation.

State as Service Provider: State of Maine providing services to build statewide cyber resilience

Key Partnerships: Counties and Maine Municipal Association play a critical role in ensuring local needs are met

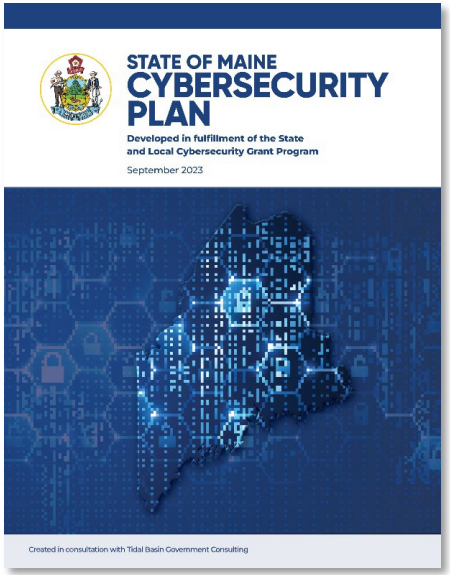
Risk-Based Approach: Strengthens rural communities' cyber resilience.

Strengthened Capabilities: Reduces cyber risk and defends against threats.

Ongoing Assessment: Annual reviews for potential plan adjustments.

State of Maine

Cybersecurity Plan – Elements



- Manage, Monitor, and Track
- Monitor, Audit, and Track
- Enhance Preparedness
- Assessment and Mitigation
- Best Practices and Methodologies
- Safe Online Services
- Continuity of Operations
- Workforce
- Continuity of Communication and Data Networks
- Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure
- Cyber Threat Indicator Information Sharing
- Leverage CISA Services
- Information Technology and Operational Technology Modernization Review
- Cybersecurity Risk and Threat Strategies
- Rural Communities

FOCUS AREAS

1. Build partnerships with counties, MMA and sector leads
2. Train local staff and raise cyber awareness
3. Deliver shared services at statewide scale
4. Reduce barriers so every community can take part

yubico MFA KEYS AND SERVICES

YubiKey is a form of Multi-Factor Authentication (MFA) that adds an extra layer of security to online accounts.

How it works: Employees input login credentials *and* plug in their YubiKey.

BENEFITS

- Crucial for enhancing security
- Significantly reduces risk of unauthorized access
- Protects sensitive information and systems from cyber threats

YUBIKEY DEPLOYMENT



Deployment Planning | **Technical Readiness** | **Lifecycle Management** | **Training and Support** | **Launch and Measurement**

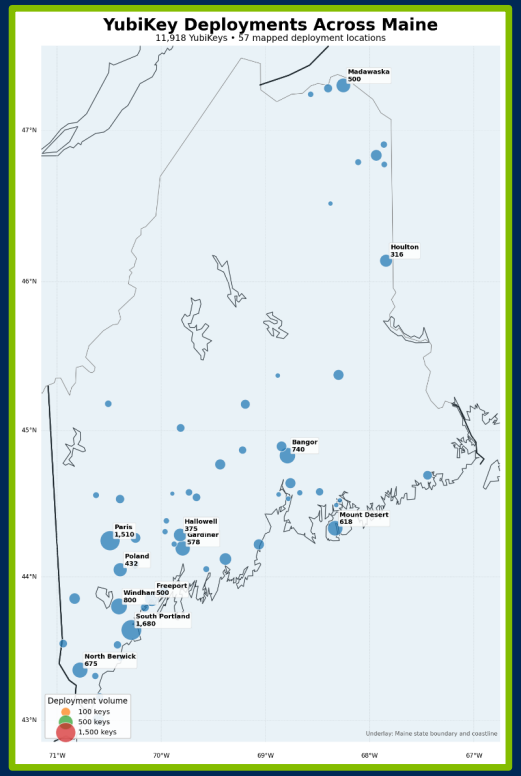
State of Maine YubiKey Deployment
Achievements under Deployments 1 & 2

Deployment #1

- Completed in 2025
- 11,472 Yubikeys were distributed statewide

Deployment #2

- Anticipated kickoff September 2026
- An additional 16,000 Yubikeys will be distributed



Results: Multi-Factor Authentication

145

entities enrolled

27,000

mfa keys procured
FY22 and FY23

0

Number of attacks stopped
by unused mfa keys

WHAT THIS MEANS FOR THE COMMUNITY

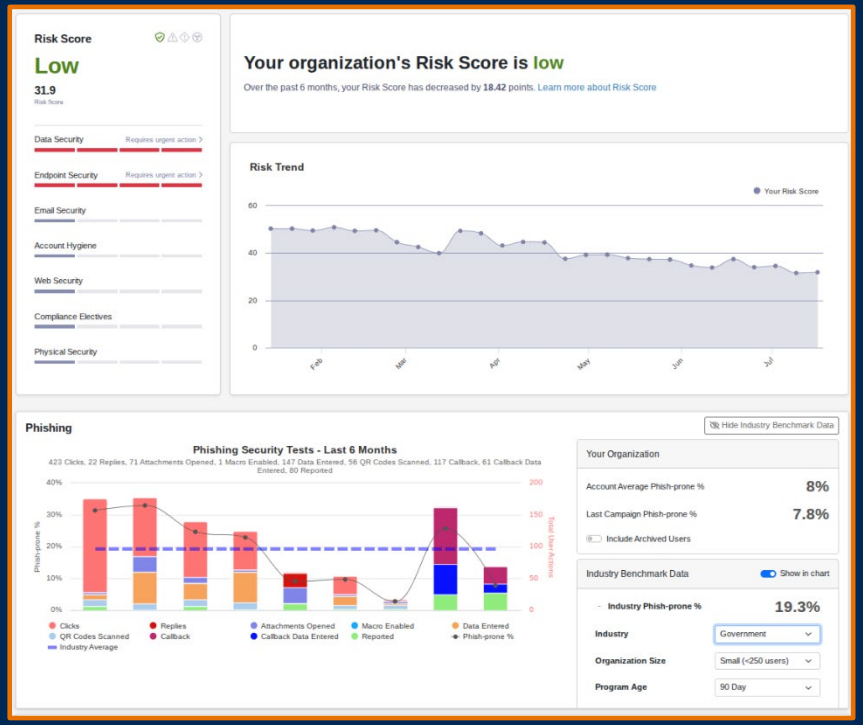
145 entities (school, towns, counties) now require MFA for email and financial systems, giving them an elevated level of security.

KnowBe4 CYBERSECURITY TRAINING PLATFORM

KnowBe4 transforms your workforce from a vulnerability into your strongest security asset

Personalized, relevant, and responsive AI-native attack simulation and training, covering topics like:

- Phishing and email security
- Social engineering attacks
- Ransomware threats
- Data protection & privacy
- Mobile device security
- Password management



nuHarbor KNOWBE4 MANAGED SERVICES

Building Security Awareness



Security Newsletters

Share simple, practical security tips and tricks to help everyone stay cyber-safe.



Security Training

Teach staff how to recognize common cyber risks and how to protect themselves.



Simulated Phishing

Send realistic but fake phishing emails to help teach staff how to spot scams in real-time.



Remedial Testing & Training

Provide an extra layer of training to staff who are tricked by the simulated phishing test.

Results: Security Awareness Training

21,000

training licenses in use

9% → 3%

phishing click rate, first test vs. latest

26-33%

2026 quarterly training completion rates

WHAT THIS MEANS FOR THE COMMUNITY

Staff are now less likely to click a phishing link that may expose you to ransomware and malware.

ATOM Group MUNICIPAL CYBER DEFENSE PROGRAM

The MCDP-Maine program will mitigate inherent risk posed by Maine's Human Intrusion Prevention Systems.

Training program was developed in response to data collected across New England and addresses critical aspects of cybersecurity

The Program

The MCDP-M program will deliver high-impact results with a four-pillar approach:

- **Role-Specific Education:** Training tailored to the specific duties of municipal and K12 staff.
- **Response & Recovery Preparedness:** Practical guidance to ensure continuity of operations during an incident.
- **Flexible Delivery:** In-person and virtual options to ensure participation regardless of geography.
- **Hands-On Exercises:** Tabletop simulations that build interagency coordination and executive decision-making.

ATOM Group

INCIDENT RESPONSE TRAINING PILOT PROGRAM



IN PERSON SEMINARS AND WORKSHOPS

Coverage Area: coastal and inland municipalities located in the Saco region and south.

LIVE-STREAMED INTERACTIVE WEBINARS

Coverage Area: state-wide.

QUARTERLY REGIONAL CYBER DEFENSE BRIEFING

Coverage Area: State-wide / Rotating

Each quarter, a different strategic location will be selected to ensure statewide physical presence.

Program Partners

































SLCGP Planning Committee

The **Planning Committee** serves as a representative voice for local input.

Representatives from:

- State, County, and Local governments
- Public Education
- Public Health
- Public Safety
- Emergency Communications
- Election Infrastructure
- The Judicial System
- Public Critical Infrastructure
- The National Guard

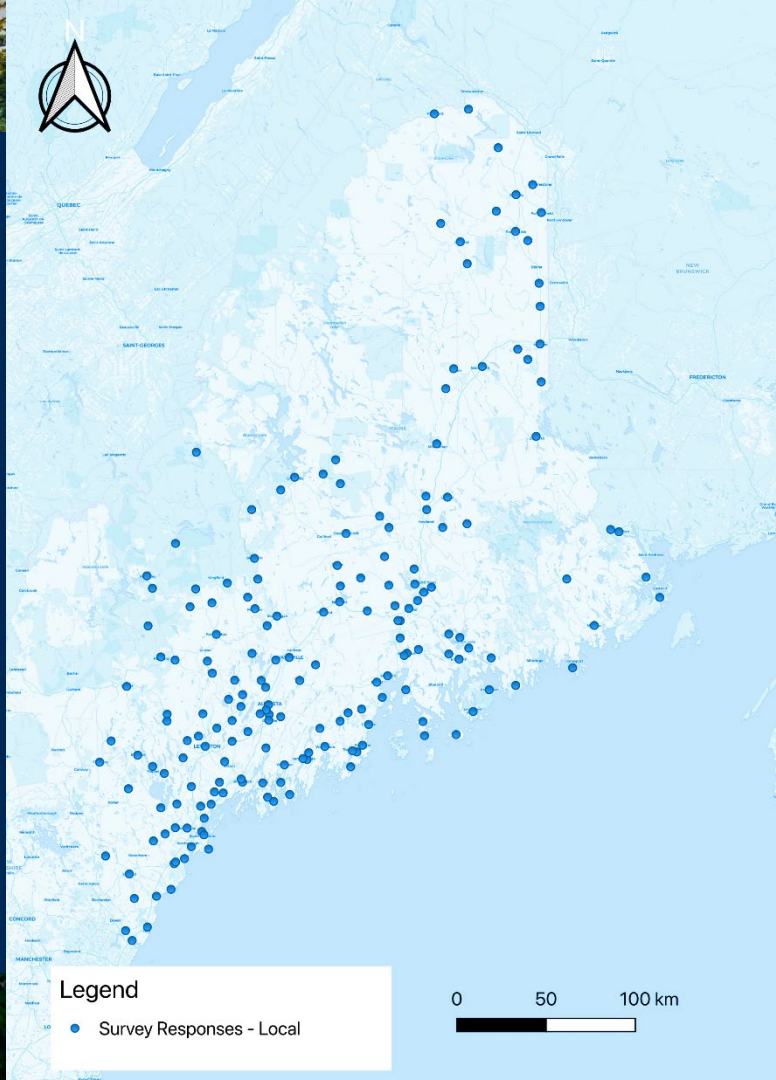


Where We've Reached

- 173 organizations take part in at least one SLCGP service
- Participants in *all 16* of Maine's counties

PARTICIPATION BY TYPE

- Municipalities: *66*
- School districts: *93*
- Counties: *11*



Map illustrates respondent areas for surveys from start of program

State of Maine

SLCGP Project Vendors

ATOM Group	• Municipal Cyber Defense Program (MCDP-M) Training program was developed in response to data collected across New England and addresses critical aspects of cybersecurity • Incident Response Training Pilot Program
Yubico	• Multifactor Authentication Keys (MFA) Annual distribution of physical keys, readiness reviews, training support, technical and operational workshops
KnowBe4	• Personalized, relevant, and responsive AI-native attack simulation and training consoles: Phishing and email security, ransomware attacks, data protection and privacy
nuHarbor Security	• Managed services for KnowBe4: Onboarding and technical support, initialization of trainings, reporting and remedial training
Michael Baker International	• Implementation of all SLCGP projects, vendor coordination, and grant support

Conclusion

We encourage all Maine entities to:

- **Participate in Maine's SLCGP initiatives:**
  - Visit https://www.maine.gov/mema/grants/state-and-local-cybersecurity-grant-program
  - Contact slcybersecurity.grant@maine.gov with general questions
- **Join the Multi-State Information Sharing and Analysis Center (MS-ISAC): 24/7 SOC support, threat intel, malicious domain blocking**
  - Register at https://learn.cisecurity.org/ms-isac-registration
- **Sign up for CISA's Cyber Hygiene Vulnerability scanning program**
  - Enroll at https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools
- **Check out the Cyber Incident Response Plan templates**
  - Distributed by Maine Educational Technology Directors Association (METDA) and Maine School Management Association (MSMA)



Questions & Discussion