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

Building a Secure Future

Webinar 1: An Overview of Maine's Cybersecurity Initiatives under Year 1 of the SLCGP

December 4, 2024

Overview

1. SLCGP Overview
2. Planning Committee
3. Cybersecurity Plan
4. Local Outreach/Integration
5. Outcomes/Goals
6. Services: KnowBe4
7. Services: YubiKey
8. Cybersecurity Resources
9. Questions

Presenters

Nathan Willigar

Chief Information Security Officer
MaineIT

Joe Legee

Deputy Director
Maine Emergency Management Agency

State and Local Cybersecurity Grant Program (SLCGP)

National Programmatic Goal

Improve cybersecurity posture of state, local, and territorial (SLT) government organizations.

Key Objectives

- Develop and implement cybersecurity plans.
- Enhance cybersecurity resilience through assessments and training.
- Encourage the adoption of best practices, such as multifactor authentication and data encryption.

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

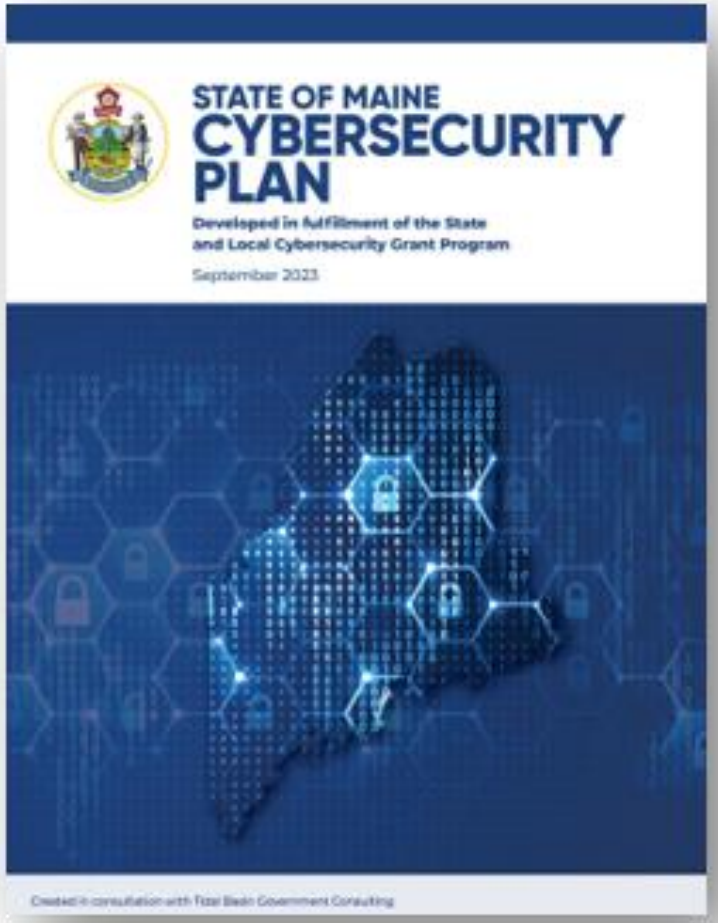
Funded by the Infrastructure Investment and Jobs Act (IIJA)

SLCGP Planning Committee

The Planning Committee serves as a representative voice for local input. It contains representatives from State, county, and local government, public education, public health, public safety, emergency communications, election infrastructure, the judicial system, public critical infrastructure, and the National Guard.

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.

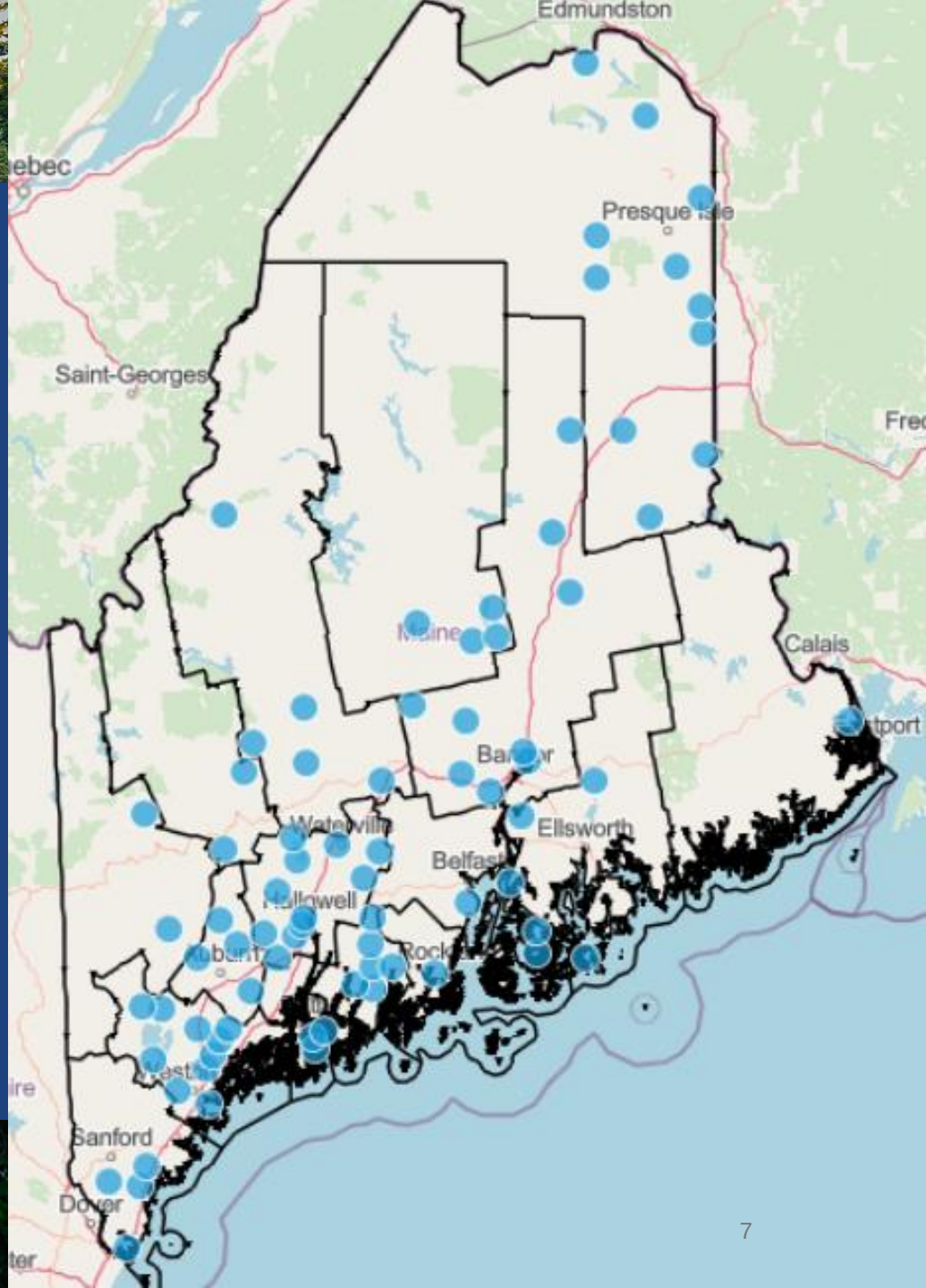
Ongoing Assessment: Annual reviews for potential plan adjustments.

Stakeholder input is an integral part of SLCGP

- Aspires to break down silos in communications
- Encourages a whole-of-state approach to address cybersecurity risks

Ways the program has incorporated local input:

- April 2023: Cybersecurity Capability Survey
- Aug 2023: Local Consent Survey
- Fall 2024: 1:1 Technical Support
- December 2024: Webinar Series

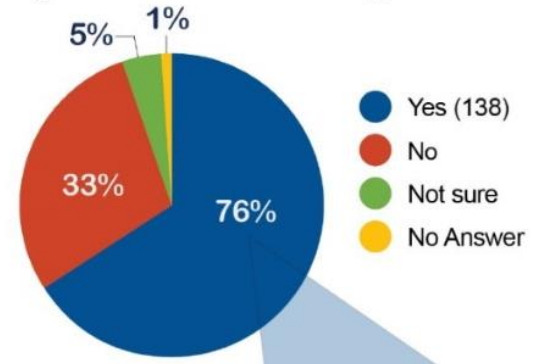


Organizations responding to the survey

181

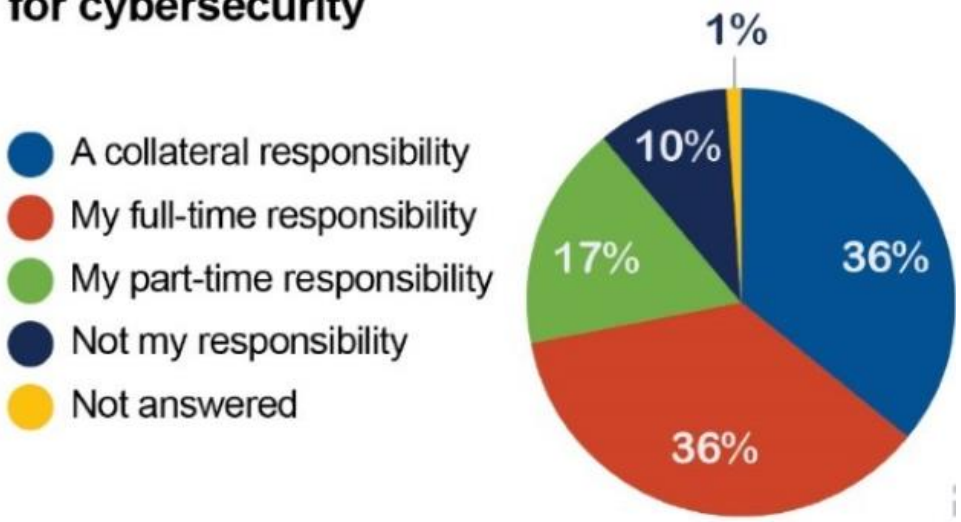
8	79	94
County	Municipality	School Districts

Organization has an IT budget



Does the IT budget address cybersecurity?

Organization has dedicated position for cybersecurity



Percentage of organizations outsourcing cybersecurity responsibilities

14% responding organizations experienced a cyber incident within the last year

Median number of personnel in organizations dedicated to cybersecurity

What will SLCGP implementation look like in Maine?

Our 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.

Our 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.

Cybersecurity Program Goals and Objectives

1. Identify, develop and maintain partnerships
2. Enable cybersecurity training and awareness activities
3. Empower local governments to leverage essential shared services
4. Execute requirements of the State and Local Cybersecurity Grant Program

SLCGP Implementation Strategies

Build and leverage partnerships

Building relationships with partners across Maine and maintaining open lines of communication with critical infrastructure sector leads to ensure a coordinated approach.

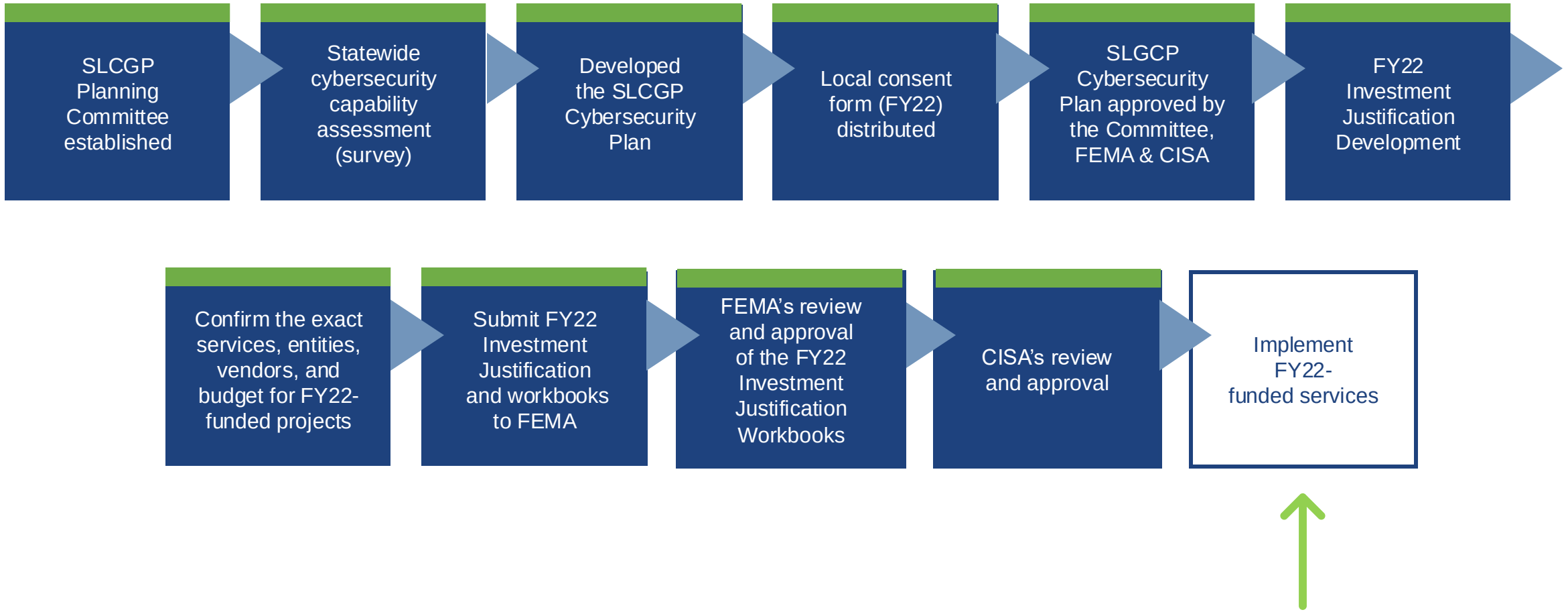
Reduce barriers

Strive to understand what barriers organizations face in implementing cybersecurity best practices and identify collective approaches to overcome them.

Increase resiliency

Build capability and capacity at the organizational level to ensure the impact of these cybersecurity initiatives is enduring and sustainable.

Status of Year 1 Funded Projects and Next Steps



SLCGP Projects: Year 1

The State of Maine intends to provide FY22 SLCGP-funded shared services to local governments.

Security Awareness Training

Providing centrally managed security awareness training for end users (employees) in qualifying entities.

Multi-Factor Authentication (MFA)

Providing MFA services to qualifying entities to implement on their networks

Cybersecurity Resources

Increasing practitioners' awareness and implementation of federally offered free and fee-based cybersecurity resources

Vendor Overview

Security Awareness Training and MFA

SLCGP-funded Shared Services

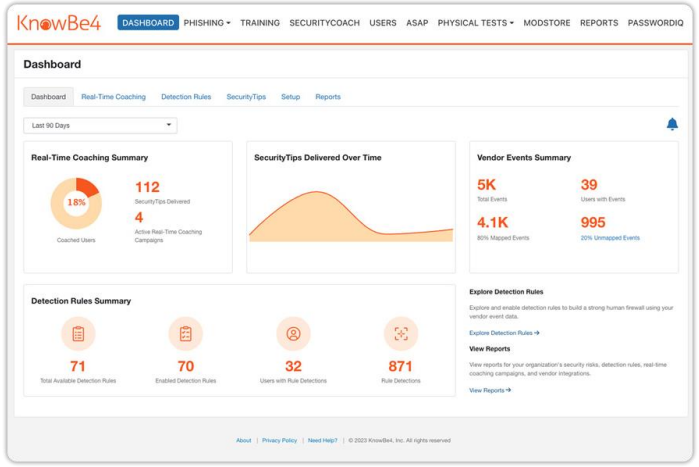
KnowBe4 Security Awareness Training

KnowBe4's content is developed by cybersecurity experts to help organizations improve overall security awareness and change user behavior.

Self-paced training sessions are delivered via their online platform through pre-recorded modules.

The training may cover a wide range of topics, including but not limited to:

- Phishing and email security
- Social engineering attacks
- Password management
- Ransomware threats
- Data protection and privacy
- Secure use of mobile devices and applications



Register today!
SLCGP Webinar 2: Security Awareness Training with KnowBe4

Thursday, Dec 12th

SLCGP-funded Shared Services

MFA with Yubico

Register today!
SLCGP Webinar 3: Multi-Factor Authentication with Yubico

Friday, Dec 13th

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.

- Multi-factor authentication (MFA) is crucial for enhancing security
- Significantly reduces risk of unauthorized access
- Protects sensitive information and systems from cyber threats

Cybersecurity Resources

We'd like to highlight the many free and fee-based cybersecurity resources that are available to local governments.

These resources will be promoted through upcoming outreach efforts, to increase awareness of these resource offerings.

Resource Links

- Center for Internet Security Resource Page
- MEMA's Cyber Security Resource Page
- MEMA's SLCGP Website
- Federal SLCGP Website (CISA)

Questions or Concerns

- Planning Committee Chair: Nicholas Marquis, Acting Chief Information Officer
- Co-Chair: Nathan Willigar, Chief Information Security Officer
- General Questions: slcybersecurity.grant@maine.gov

Additional Recommendations

We encourage organizations to:

- Join the Multi-State Information Sharing and Analysis Center and/or the Elections Infrastructure Information Sharing and Analysis Center (no cost)
- Sign up for CISA's Cyber Hygiene Vulnerability scanning program (no cost)
- Complete the National Cyber Security Review
- Participate in Maine's SLCGP offerings
- Gain familiarity with the many resource offerings through the links provided in the previous slide

Questions?