EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY

OFFICE OF GRANTS AND RESEARCH
HOMELAND SECURITY DIVISION

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

POST-AWARD TECHNICAL ASSISTANCE WEBINAR

OCTOBER 15, 2024

WEBINAR LOGISTICS

To minimize background noise, attendees are on mute

At the end of the presentation there will be a Q&A session

If you have a question during the webinar, you may put it in the "Questions" box

A copy of this presentation and a list of FAQ's with answers will be provided for attendees after the webinar

AGENDA

- Welcome
- Grant Overview
- Required Memberships, Programs, and Services
- Recommended Memberships
- State Match
- Reporting & Reimbursements
- Resources
- Questions

SPECIAL THANKS TO SECRETARY JASON SNYDER OF EOTSS, DEPUTY SECRETARY SUSAN TERREY OF EOPSS AND THE CYBERSECURITY PLANNING COMMITTEE FOR THEIR SUBJECT MATTER EXPERTISE, GUIDANCE AND SUPPORT FOR THIS PROGRAM.

OFFICE OF GRANTS AND RESEARCH (OGR) LEADERSHIP TEAM

KEVIN STANTON
EXECUTIVE DIRECTOR

CORINE PRYME
DIRECTOR OF ADMINISTRATION AND FINANCE

STEVEN DOMINGS
BUDGET MANAGER

BENJAMIN PODSIADLO
DIVISION CHIEF

KATHRYN LATIMER
DIVISION MANAGER

SARAH COOK
PROGRAM COORDINATOR

MASSACHUSETTS SLCGP GRANT PROGRAMS AWARDED IN FY24

STATE SHARE CYBERSECURITY GRANT PROGRAM (SSCGP)

State Agencies (ex. Sheriff's Office, District Attorney, etc.)

MUNICIPAL LOCAL CYBERSECURITY GRANT PROGRAM (MLCGP)

Local Units of Government (ex. Cities, Towns, School Districts, etc.)

PURPOSE OF FUNDING OPPORTUNITY

This grant was a competitive solicitation for Massachusetts state agencies and local units of government for the purpose of preventing, protecting against, mitigating, responding to, and recovering from cybersecurity threats and attacks.

To keep pace with today's cyber threat environment, local governments and entities in Massachusetts must adopt key cybersecurity best practices and advance towards a Zero Trust Architecture.

MLCGP & SSCGP AWARD OVERVIEW

130 awardees totaling $6,894,089.37

Period of Performance: Fall 2024 - June 30, 2025

The exact start date for your organization is the date your Standard Contract Form was signed by OGR's Executive Director Kevin Stanton.

We are awaiting additional guidance from FEMA on when spending can commence and will keep you updated.

Your organization may not spend any funds from your award prior to the start date of the contract.

REQUIRED MEMBERSHIPS, PROGRAMS, AND SERVICES

Subrecipients must be registered in SAM.gov, obtain a UEI#, and maintain an active registration during this grant period of performance.

Subrecipients receiving funding from this grant must comply with all of the following mandatory grant requirements:

Cyber Hygiene Services – *Required for subrecipients*

Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.

Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for the free grant required Cyber Hygiene Services, email: vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLCGP. For more information, visit CISA's Cyber Hygiene Information Page (https://www.cisa.gov/cyber-hygiene-services).

REQUIRED MEMBERSHIPS, PROGRAMS, AND SERVICES - CONTINUED

Nationwide Cybersecurity Review (NCSR) - *Required for subrecipients*

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the NIST Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.

Eligible entities and their subrecipients are required to complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. However, subrecipients receiving non-funding assistance in lieu of funding do not have to complete the NCSR.

For more information, visit Nationwide Cybersecurity Review at www.cisecurity.org.

Homeland Security Exercise and Evaluation Program (HSEEP) - *Required for subrecipients*

Exercises conducted with grant funding will be managed and conducted consistent with the Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) Homeland Security Exercise and Evaluation Program (HSEEP).

HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

RECOMMENDED MEMBERSHIPS

Subrecipients are **strongly encouraged** to become a member of the **MS-ISAC and/or EI-ISAC**, as applicable. Membership is free.

The **MS-ISAC** receives support from and has been designated by DHS as the cybersecurity ISAC for State, Local, and Territorial (SLT) governments. The MS-ISAC provides services and information sharing that significantly enhances SLT governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises. DHS maintains operational-level coordination with the MS- ISAC through the presence of MS-ISAC analysts in CISA Central to coordinate directly with its own 24x7 operations center that connects with SLT government stakeholders on cybersecurity threats and incidents. To register, please visit https://learn.cisecurity.org/ms-isac-registration. For more information, visit MS-ISAC (cisecurity.org).

The **EI-ISAC** is a collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector Government Coordinating Council. The EIISAC is funded through DHS grants and offers state and local election officials a suite of elections-focused cyber defense tools, including threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness, and training products. To register, please visit https://learn.cisecurity.org/ei-isac-registration. For more information, visit https://www.cisa.gov/topics/election-security.

MATCHING FUNDS GUIDELINES & REQUIREMENTS

Our friends at EOTSS have secured the matching funds needed for the Commonwealth to meet the required match component for this program.

As the State Administering Agency for this award, OGR will be managing these state match dollars. Therefore, each of you will be receiving additional funds so that your project can meet the federally mandated match requirement without having to dig into your own pocketbook.

NEXT STEPS

- Each subrecipient will receive an email with the exact amount of state funds you will receive. Attached will be a one-page form for you to complete and return so that you can identify how your state agency or local municipality intends to utilize the additional funds.

- Once received and approved, you will receive a separate contract or ISA to complete and return to reflect the state match award.

- Subrecipients must spend all state provided match funds prior to June 30, 2025. There are **absolutely no exceptions or extensions** for expenditure of match funds beyond June 30, 2025.

- Match funds must be tracked separately from the federal funds which is why you will be required to submit two fiscal quarterly reports each quarter (one for federal spending and one for state match spending).

STATE MATCH FORM OVERVIEW

[MLCGP Match Fund Guidelines Form]

REPORTING & REIMBURSEMENTS

Reporting Period	Due Date
Quarter 1 *Contract start date – September 30, 2024*	October 15, 2024
Quarter 2 October 1, 2024-December 31, 2024	January 15, 2025
Quarter 3 *January 1, 2025 – March 31, 2025*	April 15, 2025
Quarter 4 *April 1, 2025 – June 30, 2025*	July 15, 2025

- Quarterly Reports track activities and expenditures.

- (1) Progress Report and (2) Expenditure Workbooks (federal spending and state spending) are required each quarter.

- All Reports and supporting documents will be submitted online via Cognito. You will receive a link to Cognito along with the additional require documents.

- Please note: it is <u>required</u> that quarterly reports be submitted even if there was $0 of spending in the Quarter. Just note $0 spending on the quarterly report(s).

REPORTING & REIMBURSEMENTS - CONTINUED

- Before your first Quarterly Report is submitted, you must complete the State Match Guidelines form.

- Each reporting period you will submit two reports.
  - ✓ Part A will consist of a programmatic (progress) report and
  - ✓ Part B will consist of the financial reports (Excel Workbook) – one for federal funds and one for state funds.

- It is recommended that you use the same Excel Workbook (one per funding source) for the entire period of performance for this grant.

- Submission of these reports is required for all subrecipients.

- This is a cost reimbursement grant. Reimbursement requests must be submitted to OGR on a quarterly basis.

PROGRESS REPORT OVERVIEW

2024-2025 Municipal Local Cybersecurity Grant Program (MLCGP) Progress Report

EXPENDITURE WORKBOOK OVERVIEW

Steve Domings, OGR Budget Director

RESOURCES

Cybersecurity and Infrastructure Security Agency (CISA):
https://www.cisa.gov/

CISA's Cyber Hygiene Information Page
https://www.cisa.gov/cyber-hygiene-services

Nationwide Cybersecurity Review:
https://www.cisecurity.org/

Homeland Security Exercise and Evaluation Program (HSEEP):
https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

Information on MS-ISAC and EI-ISAC:
https://www.cisa.gov/topics/election-security

QUESTIONS

For any administrative or technical questions after the webinar please email Sarah Cook: sarah.e.cook@mass.gov