EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY

OFFICE OF GRANTS AND RESEARCH

STATE SHARE CYBERSECURITY GRANT PROGRAM

APPLICATION ASSISTANCE WEBINAR

FEBRUARY 20, 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/Introductions
- State Share Cybersecurity Grant Program
- Eligibility
- Timeline
- Allowable and Unallowable Expenses
- Application Process
- Application Review and Scoring
- Notification
- Resources
- Questions

EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY (EOPSS) LEADERSHIP

TERRENCE M. REIDY
SECRETARY

SUSAN TERREY
DEPUTY SECRETARY, HOMELAND SECURITY ADVISOR

OFFICE OF GRANTS AND RESEARCH (OGR) LEADERSHIP AND HOMELAND SECURITY DIVISION

KEVIN STANTON
EXECUTIVE DIRECTOR

SONYA SCHEY
DIVISION MANAGER

BENJAMIN PODSIADLO
DIVISION CHIEF

SARAH COOK
PROGRAM COORDINATOR

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES AND SECURITY (EOTSS) LEADERSHIP AND TEAM

JASON SNYDER

SECRETARY, COMMONWEALTH CHIEF INFORMATION OFFICER

SUSAN NOYES

DIRECTOR, MUNICIPAL AND SCHOOL IT TECHNOLOGY

MICKEY LAVICSKA

RISK MANAGEMENT AND COMPLIANCE COORDINATOR

STATE SHARE CYBERSECURITY GRANT PROGRAM (SSCGP)

Purpose: This grant is a competitive solicitation for units of state government within Massachusetts, interested in preventing, protecting against, mitigating, responding to, and recovering from cybersecurity threats and attacks.

The Office of Grants and Research (OGR) will make available approximately **$1,822,429** in funding to units of state government through the federal State and Local Cybersecurity Grant Program (SLCGP) to assist in strengthening cybersecurity while reducing systemic cyber risk.

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

ELIGIBILITY

Only a Massachusetts unit of state government (e.g., state agency, authority, or state institution of higher education) is eligible to apply.

Only one (1) application per unit of state government will be permitted.

The maximum award amount for a unit of state government is $100,000.

The **Chief Executive Officer** of the unit of state government applying for a grant award must sign the application when submitted.

TIMELINE

✓ AGF Posted: February 9, 2024

Application Due Date: March 8, 2024

Award Notification: May 2024

Period of Performance: May 2024-June 2025

ALLOWABLE AND UNALLOWABLE EXPENSES

Allowable cost categories for local equipment and technology: ✓

- Contract/Consultant (to install or train on how to use items purchased)
- Equipment and Technology (goods purchased)
- Other (identify any additional costs that directly correlate to goods purchased)

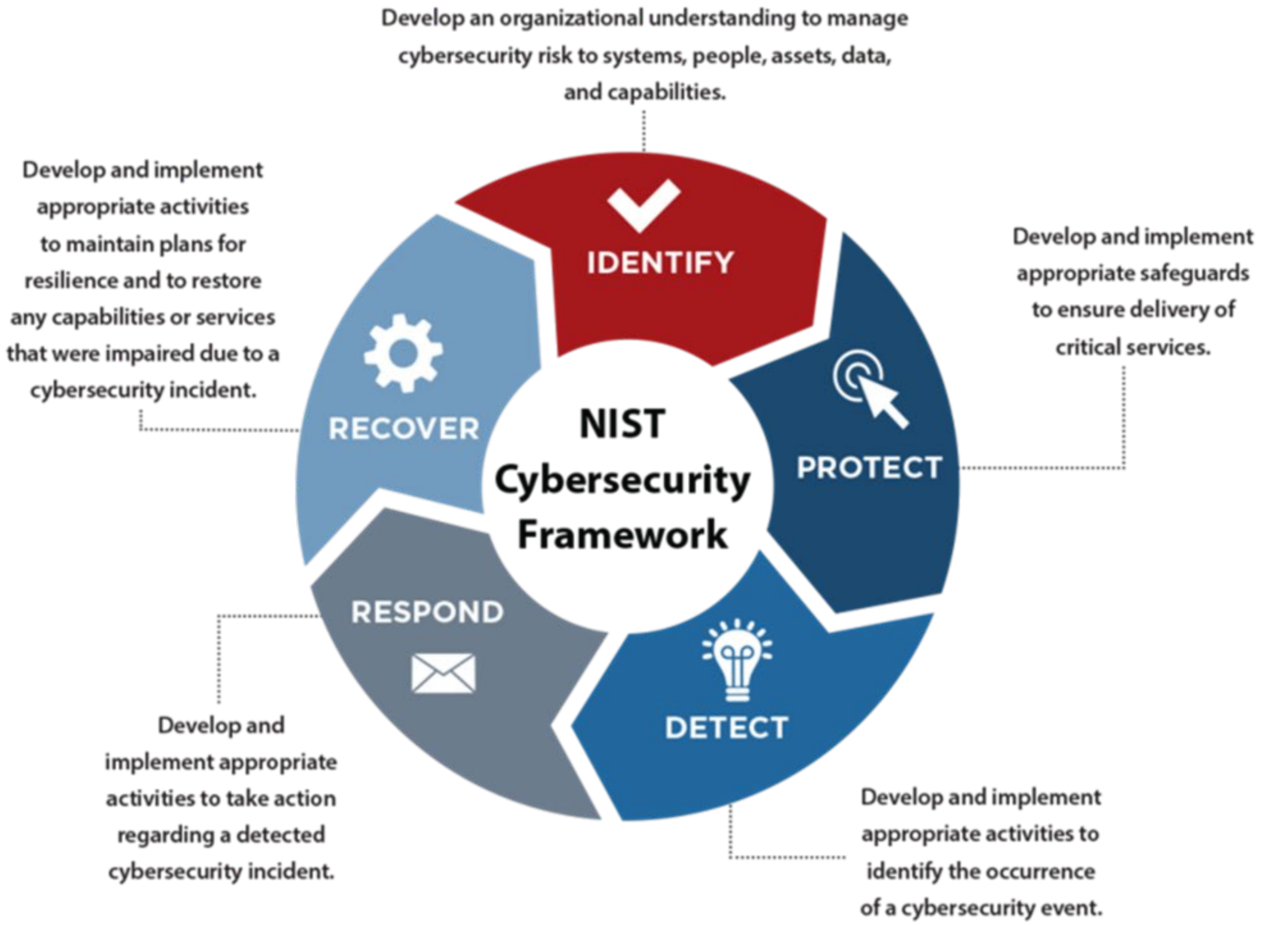
All goods and services must be in accordance with the requirements described in the AGF.

These grant funds may not be used for any of the following: 🚫

- To pay a ransom, retainer for cybersecurity services, cybersecurity insurance premiums
- For recreation or social purposes
- To acquire land or to construct, remodel, or perform alterations of buildings or other facilities

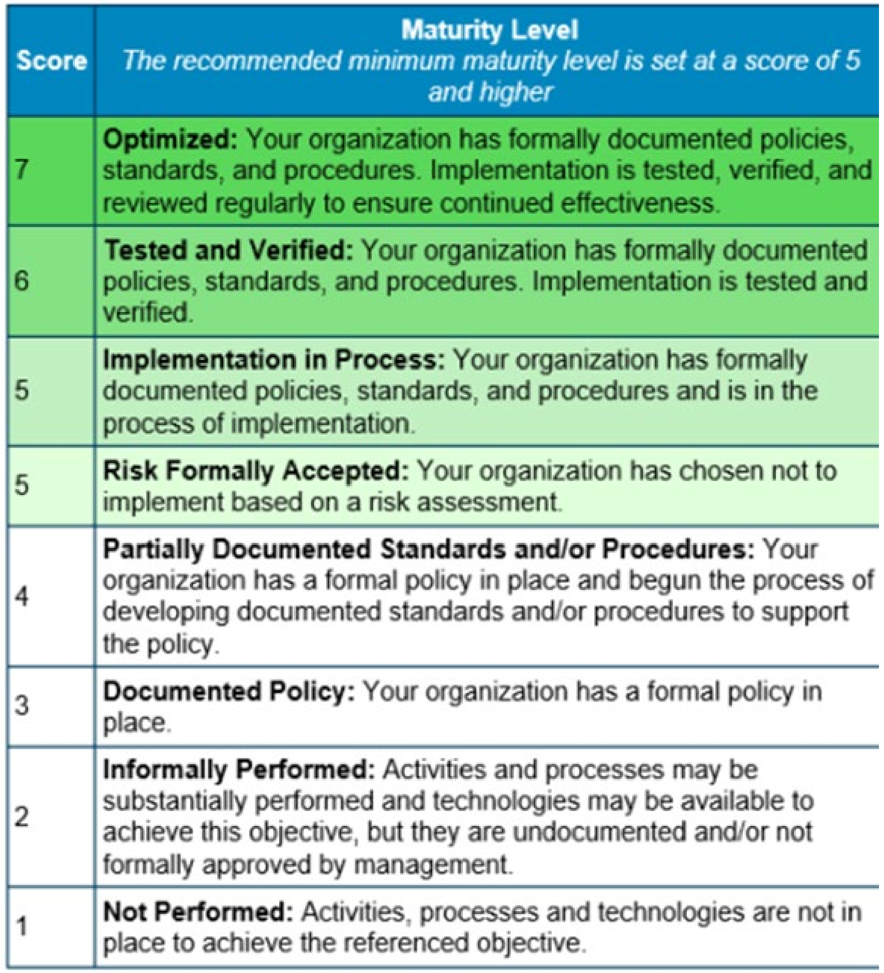
NATIONWIDE CYBERSECURITY REVIEW

The NCSR is a no-cost, anonymous, annual self-assessment. All states (and agencies), local governments (and departments), tribal nations, and territorial (SLTT) governments are required to participate. It is designed to measure gaps and capabilities of SLTT governments' cybersecurity programs and is based on the National Institute of Standards and Technology Cybersecurity Framework.


Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
IDENTIFY
Develop and implement appropriate safeguards to ensure delivery of critical services.
RECOVER
NIST Cybersecurity Framework
PROTECT
RESPOND
DETECT
Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

NIST CYBERSECURITY MATURITY MODEL

CISA recommends that organizations engage in Cyber Hygiene, a structured approach to creating an intelligent environment that reduces risk of exposure and contamination without having to consistently dedicated large expenditure on these IT processes. The more and more an organization adopts these principles the more they will be protected, as demonstrated in the maturity model below. The levels are intended to offer guidance on how organizations currently interact and coordinate both cybersecurity and operational risk management.



Score	**Maturity Level** *The recommended minimum maturity level is set at a score of 5 and higher*
7	**Optimized:** Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified:** Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process:** Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
5	**Risk Formally Accepted:** Your organization has chosen not to implement based on a risk assessment.
4	**Partially Documented Standards and/or Procedures:** Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy:** Your organization has a formal policy in place.
2	**Informally Performed:** Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed:** Activities, processes and technologies are not in place to achieve the referenced objective.

APPLICATION PROCESS

ONLINE APPLICATION (ATTACHMENT A)

Section I: Applicant Information

- **Chief Executive Officer Contact**
- **Grant Contact –** will serve as the project's point person and be responsible for receiving and responding to OGR's project related requests
- **Fiscal Contact**
- **Project Summary –** select the project objectives that your proposed project addresses
- Summary of the activities, programs, and/or equipment to be purchased if awarded grant funds

ONLINE APPLICATION (ATTACHMENT A) – CONT.

Section II: Application Narrative

- **Needs Assessment –** describe the organization that will benefit from this award, including its mission, activities, and community(s) served. Describe your organizations current unmet cybersecurity needs and related initiatives within your organization.

- **Project Description –** describe the allowable project(s) with a detailed project scope that meets the criteria of the SSCGP, describe the expected outcomes and how they will be measured, provide a brief narrative identifying how the project(s) will be sustained by the organization beyond the period of performance of the grant, briefly describe how this project will be managed including key roles and responsibilities, provide a usage plan for equipment and owners of proposed assets to be procured (if applicable).

- **Project Objectives –** describe how the proposed project(s) supports the SSCGP Project Objectives.

- **Milestones –** provide a detailed timeline that illustrates how the project(s) will be completed within the performance period to ensure adequate goals and resources are in place for completion of the proposed project(s).

APPLICATION REVIEW AND SCORING

This is a competitive grant and will be subject to a peer review process.

Applications will be reviewed and scored based on the following criteria:

- **Application Information –** Full contact information is required for all applicants **(10 points)**
- **Needs Assessment –** Describe the organization that will benefit from this award including current unmet cybersecurity needs and related initiatives within your organization **(15 points)**
- **Project Description –** Describe allowable projects, expected outcomes and how they will be measured, identify how the project(s) will be sustained by the organization, management of project (key roles, responsibilities, personnel), usage plan for equipment **(25 points)**
- **SSCGP Project Objectives** – Provide a detailed description of how the proposed project(s) supports the SSCGP Project Objectives **(10 points)**
- **Milestones** – Provide a detailed timeline that illustrates how the project(s) will be completed within the performance period **(15 points)**
- **Budget Narrative & Budget Details –** Provide a brief narrative of what the proposed budget entails (including how to budget was determined and budget cost-effectiveness), as well as an accurate budget breakdown by cost category, cost, and description of expenditure **(25 points)**

ONLINE APPLICATION (ATTACHMENT A) – CONT.

Section III: Budget

- **Funding Amount Requested**
  - ➢ Only one (1) application per unit of state government will be permitted
  - ➢ The maximum amount of funding requested per application is $100,000

- **Budget Narrative Summary –** provide a summary of what the proposed budget entails, including how the budget was determined and cost effectiveness, as well as an accurate budget breakdown by allowable cost category, cost, and description of expenditure

- **Attachment B: Budget Excel Worksheet**
  - ➢ Please be sure to complete <u>all</u> Excel tabs of the template provided and upload it with your application.

- **OGR Subrecipient Risk Assessment Form**

ATTACHMENT B REVIEW WITH FISCAL

MASSACHUSETTS STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP) PLAN

This document is **FOR OFFICIAL USE ONLY (FOUO)** and not for public use or dissemination. Do not share or forward without permission from OGR.

Please contact Sarah Cook at sarah.e.cook@mass.gov to obtain a copy for your use in creating your application.

All requests for the MA SLCGP Cybersecurity Plan will be vetted.

If you have any questions regarding this requirement, please contact Sarah Cook at sarah.e.cook@mass.gov

APPLICATION SUBMISSION

This is a TWO step process:

Step 1. Electronic Submission
Step 2. Hard Copy Submission

Please note: Submission of the online form alone will not be accepted as an application submission. All applicants are required to also submit a signed hard copy of the complete application.

Both applications (electronic and hard copy) are to be submitted on or before Friday, March 8, 2024, at 4:00pm. Emailed submissions will NOT be accepted.

APPLICATIONS SUBMITTED AFTER 4 P.M. on MARCH 8, 2024, WILL NOT BE ACCEPTED

STEP 1: ELECTRONIC SUBMISSION

1. Complete the step-by-step online form as per instructions.

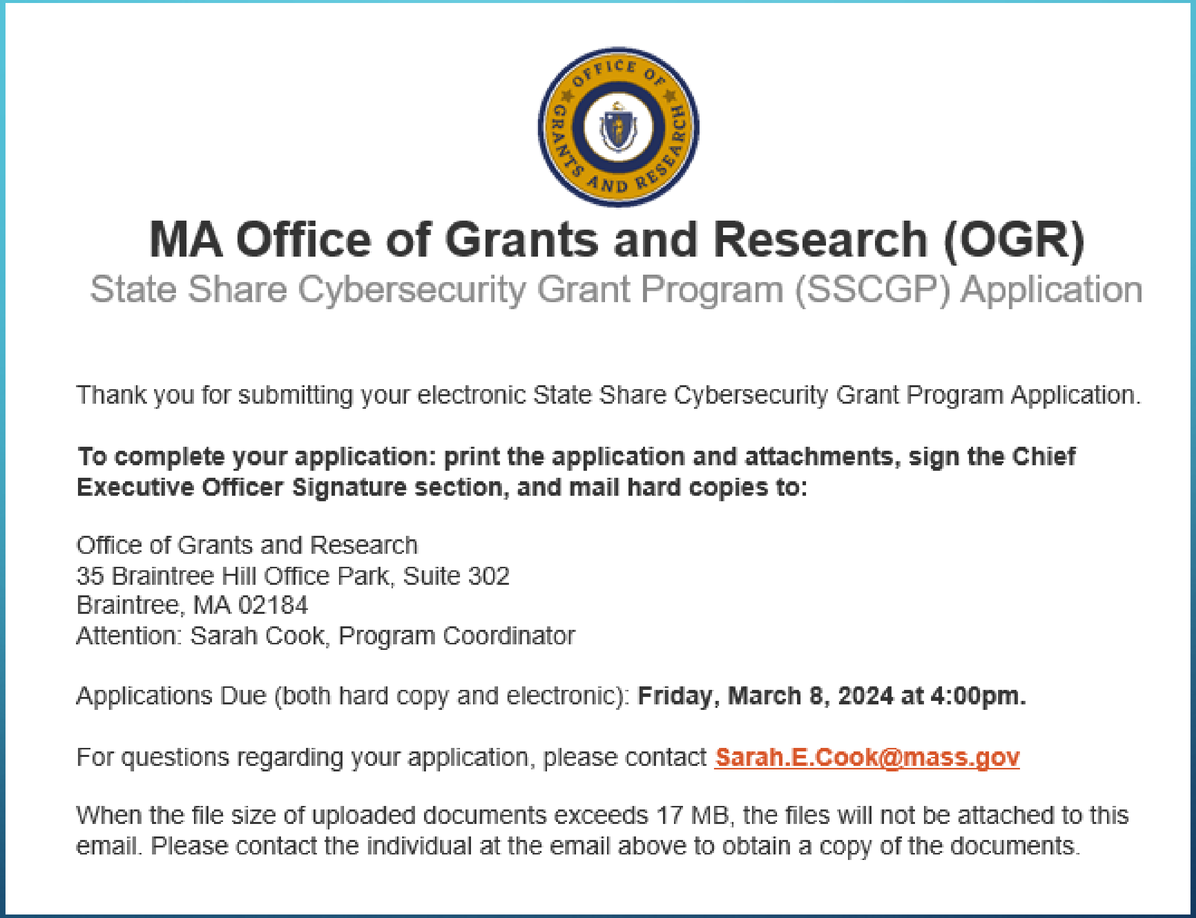
2. Upload Attachment B, the Budget Excel Workbook. The online application must be completed and submitted with the uploaded Excel document.

3. Press the "submit" button to submit your application.

4. You will then receive a confirmation email with a copy of your application.

The form and attachments are to be submitted electronically via the online application process on or before Friday, March 8, 2024, at 4:00pm.

ELECTRONIC SUBMISSION CONFIRMATION



MA Office of Grants and Research (OGR)

State Share Cybersecurity Grant Program (SSCGP) Application

Thank you for submitting your electronic State Share Cybersecurity Grant Program Application.

To complete your application: print the application and attachments, sign the Chief Executive Officer Signature section, and mail hard copies to:

Office of Grants and Research
35 Braintree Hill Office Park, Suite 302
Braintree, MA 02184
Attention: Sarah Cook, Program Coordinator

Applications Due (both hard copy and electronic): **Friday, March 8, 2024 at 4:00pm.**

For questions regarding your application, please contact Sarah.E.Cook@mass.gov

When the file size of uploaded documents exceeds 17 MB, the files will not be attached to this email. Please contact the individual at the email above to obtain a copy of the documents.

STEP 2: HARD COPY SUBMISSION

Upon submission of your online application, the grant contact will receive an email confirmation with the PDF attachments of the online submission. Please print these attachments and obtain the signature of the Senior Organization Official on the hard copy application.

Applicants must submit by mail:

- Online Application (Attachment A): Complete/Signed/Printed Application
- Attachment B: Budget Worksheet (Summary and Detail Sheets)

A hard copy of the application and documents must be postmarked or hand delivered by March 8th to:

Office of Grants and Research
35 Braintree Hill Office Park, Suite 302
Braintree, MA 02184
Attention: Sarah Cook, Program Coordinator

Hard copy applications should be postmarked on or before Friday, March 8, 2024, at 4:00pm.

NOTIFICATION

Once funding decisions are approved, OGR is responsible for administering and managing all contracts awarded. OGR anticipates it will announce awards under this program in **May 2024**.

RESOURCES

State Share Cybersecurity Grant Program AGF and Application:

https://www.mass.gov/info-details/state-share-cybersecurity-grant-program

Homeland Security Exercise and Evaluation Program (HSEEP):

https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

Nationwide Cybersecurity Review:

https://www.cisecurity.org/

Cybersecurity and Infrastructure Security Agency (CISA):

https://www.cisa.gov/

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