Executive Office of Public Safety and Security
Office of Grants and Research

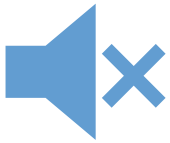
Cybersecurity Incident Response Plan and Tabletop Exercise Grant Opportunity

Application Assistance Webinar
September 16, 2025

KEVIN STANTON, EXECUTIVE DIRECTOR

KATHRYN LATIMER, DIVISION MANAGER

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” chat box

A copy of presentation materials will be provided for attendees after the webinar

Agenda

- Welcome
- CIRPTE Grant Opportunity
- Eligibility
- Timeline
- Required and Recommended Memberships
- Allowable and Unallowable Expenses
- Cost-Match Overview
- Application Process
- Resources
- Q&A

Cybersecurity Incident Response Plan and Tabletop Exercise (CIRPTE) Grant Opportunity

The **Office of Grants and Research** (OGR) is pleased to announce approximately **$1,000,000** in federal and state funds for **Massachusetts State Agencies** to develop a cybersecurity **Incident Response Plan** (Cyber IRP) or implementation of a **Tabletop Exercise** (TTX) to assist in strengthening cybersecurity while reducing systemic cyber risk.

Purpose: This opportunity is a competitive solicitation for Massachusetts State Agencies who have yet to develop a Cyber IRP or are in need of testing an existing Cyber IRP via a TTX.

The overall goal of this grant opportunity is to assist State Agencies with improving cybersecurity by reducing susceptibility to cybersecurity threats, reducing vulnerabilities, and mitigating the consequences of attacks.

Eligibility

- ✓Only a **Massachusetts State Agency (including independent/quasi-public agencies, district attorney offices and sheriff departments)** is **eligible to apply** under this grant opportunity.
  - *Local municipalities, nonprofit organizations and private vendors are **NOT** eligible to apply under this competition.*
- ✓The **Chief Executive Officer** of the state agency applying must sign the application when submitted and only one (1) application per state agency is permitted for consideration of funding.
- ✓An applicant ***must*** choose one of the eligible projects – either development of a CIRP or implementation of a TTX.

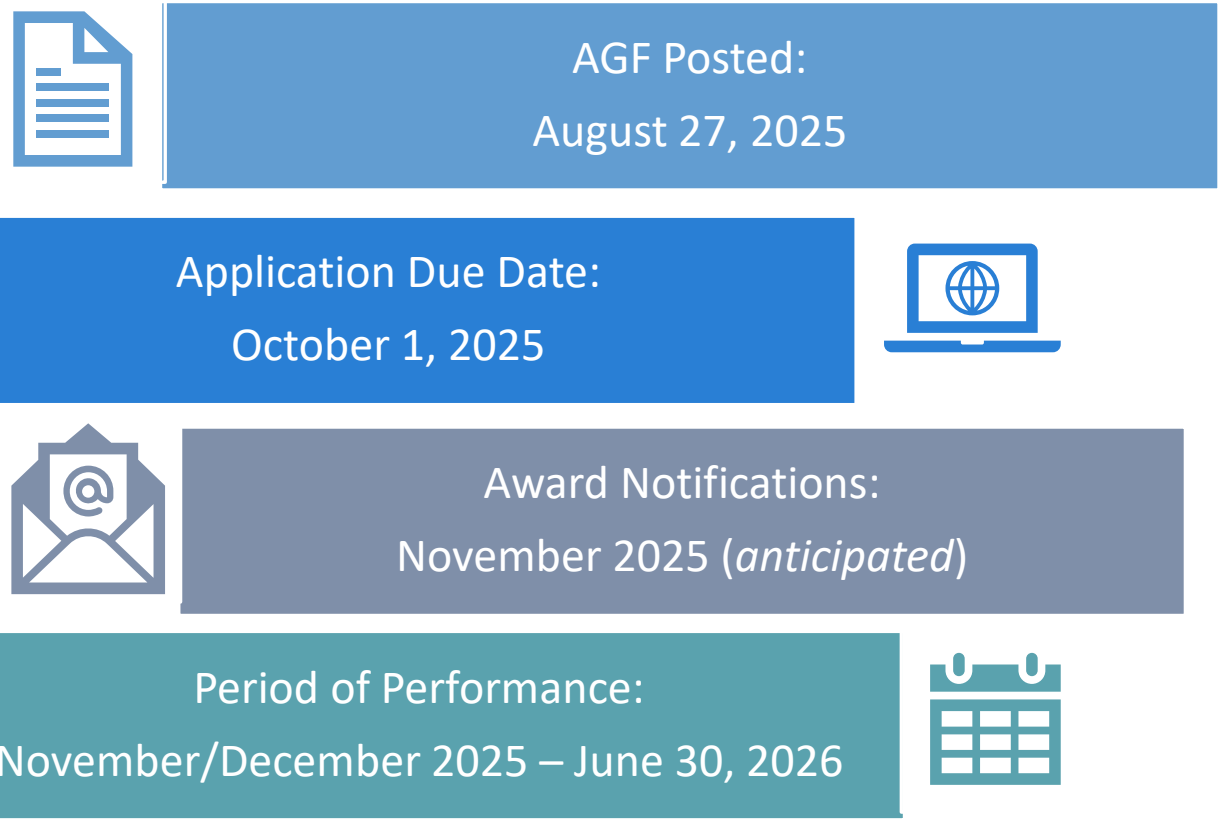
Projects and Vendors

- The only projects permitted under this grant opportunity are to develop a cybersecurity **Incident Response Plan (Cyber IRP)** or implementation of a **Tabletop Exercise (TTX).**

- Applicants awarded funds under this AGF will be required to utilize vendor(s) already secured by the Commonwealth through a competitive solicitation.

The following link will direct you to a list of eligible vendors approved for use with these funds: COMMBUYS

Timeline


AGF Posted:
August 27, 2025
Application Due Date:
October 1, 2025
Award Notifications:
November 2025 (*anticipated*)
Period of Performance:
November/December 2025 – June 30, 2026

Required Memberships, Programs, and Services

Unique Entity Identifier (UEI) # and register in the System for Award Management (SAM.gov)

Subrecipients must:

1. Obtain a UEI#
2. Be registered in SAM.gov before application submission

Please note: subrecipients do not need to have a valid UEI at the time of application; however, they must have a valid UEI in order to receive a subaward.

Cyber Hygiene Services

Service that assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.

Homeland Security Exercise and Evaluation Program (HSEEP)

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).

Nationwide Cybersecurity Review (NCSR)

Free, anonymous, annual self-assessment designed to measure gaps and capabilities of a State, Local, and Territorial (SLT) governments cybersecurity programs.

Recommended Memberships

Multi State-Information Sharing and Analysis Center (MS-ISAC):

- Provides services and information sharing that significantly enhances SLT (State, Local, and Tribal) 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 24/7 operations center that connects with SLT government stakeholders on cybersecurity threats and incidents.
- To register visit: https://learn.cisecurity.org/ms-isac-registration

Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):

- A collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector Government Coordinating Council.
- The EI-ISAC 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 visit: https://learn.cisecurity.org/ei-isac-registration

Allowable Costs

Cost Categories	Description
Contract/Vendor Costs	EOTSS has secured two vendors to perform these services for applicants selected for an award. More information about the vendors secured by EOTSS can be found on **COMMBUYS** . Recipients **must** select a vendor on the list to conduct all grant funded services for their approved project. Awardees will not be permitted to utilize a different vendor.
Other	Supplies needed to implement a TTX if not included in the vendor cost, dissemination costs associated with reproducing the CIRP developed, etc.
Indirect Costs	Federally negotiated and approved rate for costs that are not readily assignable to a particular project but are necessary to the operation or maintenance of the organization and performance of the project. **Please note:** Applicants must include a copy of the federally approved rate with the proposal.

Unallowable Costs

These grant funds are only for the development of a Cybersecurity Incident Response Plan and implementation of a Tabletop Exercise.

Any costs not directly related to these tasks will be considered **unallowable**.

Unallowable costs include:

- Agency personnel, rent, and other related administrative costs;
- Equipment and technology;
- Retainer fees; and
- Food or catering services.

Cost-Match Requirement

For this grant program, FEMA requires that eligible entities meet a cost-match requirement. **To meet this requirement, the Commonwealth of Massachusetts is providing this cost-match for subrecipients.**

This means that your award will be comprised of both state and federal funds.

Cost-Match Requirement – Cont.

Awarded applicants will receive two Interdepartmental Service Agreement (ISA) forms – one for the federal award amount and one for the state provided match amount.

The two ISAs will total the amount of funds requested; however, you must ensure that ***all*** costs requested are allowable.

Cost-Match Requirement – Cont.

Please note: **we require that the state matching funds must be spent first** to ensure all state match funds are expended by **June 30, 2026**.

State agency subrecipients are **NOT** responsible for providing the match unless they fail to spend the state match funds provided.

Application Process

Applicants may only apply for one (1) of two (2) eligible projects, either:

1. Development of a Cybersecurity Incident Response Plan (CIRP)
2. Implementation of a cybersecurity Tabletop Exercise (TTX)

There is a maximum award amount of **$40,000** for development of a CIRP and a maximum award amount of **$30,000** for a TTX.

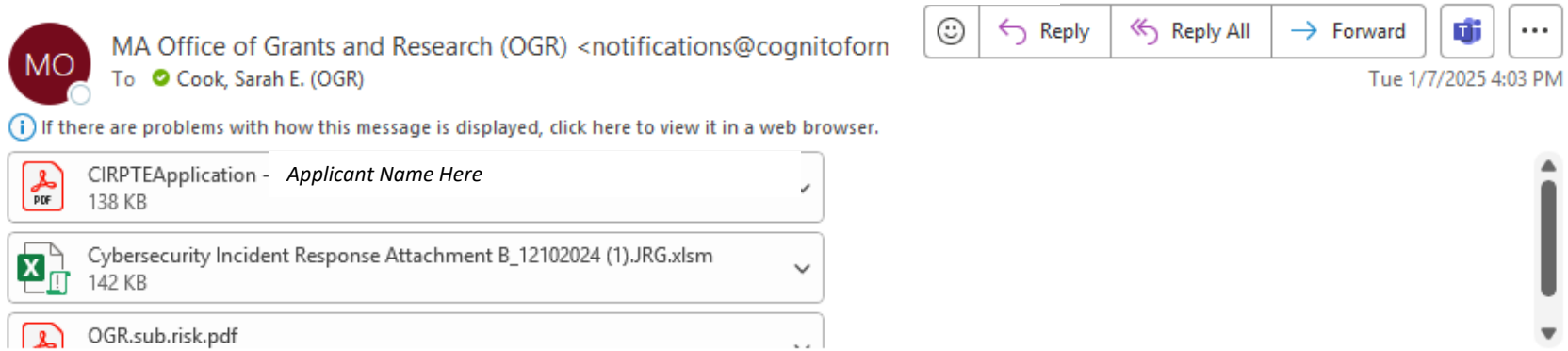
Documents required to submit with online application:

- ✓ Attachment B – Budget Worksheet
- ✓ OGR Subrecipient Risk Assessment Form
- ✓ Indirect Cost Rate Agreement – *only if indirect costs are included in your budget*

Grant Opportunity information and required application documents can be found on our website here: https://www.mass.gov/info-details/cybersecurity-incident-response-planning-and-tabletop-exercise-grant-opportunity

After you submit your application, you will receive an email with a PDF copy of the completed application and any documents you included as with the application.

CIRPTE - *Applicant Name Here*



CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

MA Office of Grants and Research (OGR)

2024 Cybersecurity Incident Response Plan and Tabletop Exercise (CIRPTE) Grant Program Application

Applicant Name Here has submitted their application.

Application Form Overview

2025 Cybersecurity Incident Response Plan and Tabletop Exercise (CIRPTE) Grant Program Application

Attachment B Review

CIRPTE Budget Workbook

Resources

CIRPTE AGF and Application Materials:
https://www.mass.gov/info-details/cybersecurity-incident-response-planning-and-tabletop-exercise-grant-opportunity

SAM.gov:
https://sam.gov/entity-registration

Cyber Hygiene Services:
https://www.cisa.gov/cyber-hygiene-services

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

Nationwide Cybersecurity Review (NCSR):
https://www.cisecurity.org/ms-isac/services/ncsr

Information on MS-ISAC:
https://www.cisecurity.org/

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

Q&A

For any administrative or technical questions after the webinar, please email:

Sarah Cook: sarah.e.cook@mass.gov
and
Ira Berberaj: ira.berberaj@mass.gov