Commonwealth of Massachusetts
Executive Office of Public Safety and Security
Office of Grants and Research
Notice of Availability of Grant Funds

Cybersecurity Incident Response Planning and Tabletop Exercise Grant Opportunity

For Massachusetts State Agencies Only

Maura T. Healey
Governor

Kimberley L. Driscoll
Lieutenant Governor

Terrence M. Reidy
Secretary

Kevin J. Stanton
Executive Director

Notice of Availability of Grant Funds (AGF)
Office of Grants and Research

August 27, 2025

Cybersecurity Incident Response Planning and Tabletop Exercise
For Massachusetts State Agencies

Applications Due: October 1, 2025, at 4:00 p.m.

Overview

In partnership with the Executive Office of Technology Services and Security (EOTSS) and Executive Office of Public Safety and Security (EOPSS), 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. To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, Massachusetts State Agencies must adopt key cybersecurity best practices, take decisive steps to modernize their approach to cybersecurity, and advance toward a Zero Trust Architecture.

OGR is the State Administering Agency (SAA) for federal funds received from the U.S. Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA). This opportunity is being supported from the federal DHS/FEMA **State and Local Cybersecurity Grant Program (CFDA# 97.137)** and with matching state funds provided by the Healey-Driscoll Administration.

Applicant 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. 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. Local municipalities, nonprofit organizations and private vendors are **NOT** eligible to apply under this competition.

Purpose

This opportunity is a competitive solicitation for Massachusetts State Agencies who have yet to develop a **Cyber IRP** or 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 by enhancing specific cybersecurity capabilities. 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

Key Dates

Key Activities	Key Dates
AGF Posted	August 27, 2025
Application Assistance Webinar (Optional)	Tuesday, September 16th, at 11 a.m. Please register here for the Application Assistance Webinar informational session. After registering, you will receive a confirmation email containing information about joining the webinar.
Application Due Date	**4:00 p.m. Wednesday, October 1, 2025**
Award Notification *(anticipated)*	November 2025
Performance Period	Tentative-November/December 2025 – June 30, 2026,

Application Requirements

Applicants are required to propose a project that addresses one (1) of the two (2) cybersecurity priority objectives as detailed below in this AGF. Applicants may select only one (1) of the priority objectives for a project funding request. Applications proposing more than one (1) project or objective or proposing to address an objective not allowed in this AGF will not be considered for funding.

Allowable Priority Objectives

Applicants must select one **(1)** of the following priority objectives **(Cyber IRP or TTX)** to be considered for funding under this grant opportunity**.**

Please select a vendor through COMMBUYS for the development of a written cybersecurity incident response plan (Cyber IRP) or to implement a TTX. The TTX should involve cross-functional staff members, including senior leadership members from the applicant's agency, to exercise, test, and refine the existing cyber-IRP for the applicant's agency.

Application Priorities

Include a detailed explanation of:

- The intended use(s) of funds provided under the grant and how the activities funded under the grant will meet the purpose.
- Include an assurance that the applicant will maintain and report all data, records, and programmatic and financial information that OGR may reasonably require.

Include a certification within your application that:

- The programs to be funded by the grant meets all the requirements of this AGF,
- All the information contained in the application is true and correct.
- The applicant will comply with all provisions of this AGF and all other applicable State and Federal laws.

Maximum Award Amount

A MASSACHUSETTS STATE AGENCY may not request more than:

- **$40,000.00** for the development of a **Cyber IRP;** or
- **$30,000.00** for a **TTX**.

Project Duration

Awards will be approximately **8 months in duration** with an **end date of June 30, 2026**.

State Match and Federal Funding Disbursement

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.** Awarded applicants will receive two Interdepartmental Service Agreement (ISA) forms to sign as subrecipients. One ISA will represent the federal funds awarded and the second ISA will represent the mandatory state match requirement of funds. The two ISAs will equal the total amount of the award approved by OGR.

All state matching funds being provided by the Commonwealth as part of an applicant's total award request must be utilized by June 30, 2026. State match funds are **use or lose by June 30, 2026**. An applicant failing to spend the state match contribution on or before that date will be required to provide their own matching funds and submit supporting documentation to prove the match requirement was met. Failure to do so may result in termination of this award and return of funds.

Subrecipient Requirements

Subrecipients must abide by all state and federal grant requirements including those listed below, as well as all OGR Subrecipient Grant Conditions which will be provided at the time awards are made. Additional information about federal grant requirements (2 C.F.R. Part 200) can be found on the 2CFR website.

Obtain a Unique Entity Identifier (UEI) and Register in the System for Award Management (SAM)

Each applicant, unless they have a valid exception under 2 CFR 25.110, must adhere to the following:

- Registered in SAM.Gov prior to application submission.
- Provide a valid UEI in its application.
- Maintain an active SAM registration with current information throughout the Federal Award process.

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

Applying for an award under this program is a multi-step process and requires a significant time commitment. Applicants are encouraged to register early as the registration process can take four weeks or more to complete. Therefore, registration should be done in sufficient time to ensure it does not impact the applicant's ability to obtain funding and/or meet required deadlines.
All entities wishing to do business with the federal government must have a UEI. The UEI number is issued by the SAM system. Requesting a UEI using SAM.gov is straightforward; the link can be found on the SAM entity registration page.

Required Memberships, Programs, and Services

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, 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.

Cyber Hygiene Services is a free service and is required for all subrecipients of this grant. To register for this service, 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.

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). Please see HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning.

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 Multi-State Information Sharing and Analysis Center (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 the Nationwide Cybersecurity Review.

Recommended Membership

Multi State-Information Sharing and Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):
Additionally, if awarded, 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 24/7 operations center that connects with SLT government stakeholders on cybersecurity threats and incidents. To register, please visit the MS-ISAC registration page. 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 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, please visit the MS-ISAC registration page. For more information, visit CISA's Election Security page.

Other Requirements

Grant Administration and Management

- Submission of satisfactory and timely quarterly progress reports and quarterly financial reports with all required back-up documentation.
- Cooperation during OGR monitoring endeavors, including site visits and desk reviews.
- Supplanting of funds is strictly prohibited. Funds for programs and services provided through this grant are intended to supplement, not supplant, other funding sources.
- All costs paid with grant funds must be direct and specific to this opportunity.
- Subrecipients must accept their award no later than 30 days from the award date. Failure to accept a grant award within the 30-day timeframe may result in a loss of funds.

Procurement

- The Commonwealth has secured two vendors to perform these services for state awardees to utilize with these state match and federal funds. As noted on page 3., applicants must select a vendor (found here: COMMBUYS) to conduct all grant funded services for their approved project. **Awardees will not be permitted to utilize a different vendor.**

Other Conditions

- In addition to the requirements set forth above, subrecipients are required to agree to and abide by all rules, regulations, and conditions pertaining to the receipt, administration, and management of state and federal grant funding.
- All costs charged to this award must comply with the rules found throughout this AGF, the federal Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200. Costs must be incurred, and products and services must be delivered within the period of performance of the award.

Reporting Alleged Waste, Fraud, and Abuse

It is the responsibility of the subrecipient to report alleged Fraud, Waste, or Abuse, including any alleged violations, serious irregularities, sensitive issues, or overt or covert acts involving the use of public funds in a manner not consistent with statutes, related laws and regulations, appropriate guidelines, or purposes of the grant. If you have information about instances of fraud, waste, abuse, or mismanagement involving DHS programs or operations, you should contact the U.S. Department of Homeland Security Office of Inspector General Hotline at 1-800-323-8603, by fax at 202-254-4297, or report online.

Evaluation Criteria and Scoring Process

Application proposals will be evaluated based on the criteria listed below. It is important that proposals clearly and completely address these requirements.

1. **Applicant Information (10 points maximum)**

2. **Needs Assessment (35 points maximum):**

    - Describe the state agency that will benefit from this award, including its mission, number of personnel, and its services to the Commonwealth, including any emergency response, public utility, social service, and financial transaction systems or services.

- If seeking a Cyber IRP, describe why it has not been previously developed or in need of updating to meet Commonwealth standards.
- If seeking a TTX, describe why a TTX hasn't been conducted thus far.
- Provide details about how this grant funding will help address cybersecurity risks and cybersecurity threats to the information systems owned or operated by or on behalf of the applicant.
- Provide detail on how the applicant's staff, stakeholders, and the public will benefit from either the applicant's proposed Cyber IRP development project or the TTX of the applicant's Cyber IRP project.
- Describe existing/related cyber initiatives within the applicant's state agency (if applicable). If not applicable, please indicate this in your application.

3. Project Description (25 points maximum):

- Describe the allowable project with a detailed project scope that meets the criteria of the allowable project objective: either development of a Cyber IRP or a TTX to test the applicant's Cyber IRP.
- Describe the expected outcomes within the performance period and how those outcomes will be measured.
- Provide a brief narrative identifying how the project will be sustained by the applicant in the future, after the period of performance has ended.
- Briefly describe how this project will be managed, including identification of key personnel, roles, and responsibilities.
- Describe how the applicant's project supports or improves the emergency response, utilities, social services, and/or financial transaction systems, if any, the applicant provides to the public.

4. Milestones (15 points maximum):

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

5. Budget Narrative & Budget Details (15 points maximum):

- A brief narrative 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.
- Applicants must describe in their budget narrative how the associated cost(s) will enhance their agency's public emergency response, utility, social service, and/or financial transaction systems or services.
- In addition to providing the budget narrative and details in Attachment A, applicants are required to complete the Attachment B (Excel) Budget Workbook. **Applicants must also complete a Budget Excel Worksheet (refer to Attachment B). Please be**

sure to complete both the Summary sheet and Detail worksheet (Excel tabs) and submit with your application.

Review Process

This is a competitive grant and will be subject to a peer review process. It is the intent of OGR to distribute funding to eligible state agencies of the Commonwealth. All applications will be reviewed and scored by a panel of three (3) reviewers. The OGR Executive Director or his designee will present the award recommendations to the Secretary of EOTSS and the Deputy Secretary of EOPSS prior to forwarding to the Governor's Office for final approval.

In addition, per federal rules and regulations, all subrecipient projects approved by OGR will be submitted to FEMA for approval. OGR reserves the right to award additional proposals recommended for funding by the peer reviewers if more funds become available after the initial awards are made.

Allowable Costs

Allowable Budget Cost Categories	Description
Contract/Vendor Costs	Eligible vendors from which awardees may select to procure the services for an approved and allowable project under this AGF can be determined via this link to COMMBUYS.
Other Costs	Supplies needed to implement a TTX if not included in the vendor cost, dissemination costs associated with reproducing the Cyber IRP plan developed, etc.
Indirect Costs	Expenses necessary for the organization's operations.

Unallowable Costs

These grant funds are only for the development of a Cyber IRP and implementation of a Cyber TTX. Any other costs not directly related to these tasks will be considered unallowable. Unallowable costs include but not limited to:

- Agency personnel, rent, grant writers and other related administrative costs
- Equipment
- Food or catering services

OGR will utilize the Sub-Grantee Risk Assessment Form during its review process to help identify whether additional monitoring plans and/or special conditions are required. OGR is required to evaluate each applicant's risk of non-compliance with Federal statutes, regulations, and

the terms and conditions of a sub-award for the purpose of determining appropriate monitoring described in 2 CFR 200.331(b).

Notification of Awards

Once funding decisions are approved, OGR is responsible for administering and managing all subrecipients. OGR anticipates it will announce awards in November/December 2025. Please note, the Commonwealth will be providing the state matching funds required by FEMA for all projects supported under this competition.

Submission Process and Deadline

Please review the following instructions carefully when submitting the Application, Budget, and other documents.

Electronic Submission

Submit your Online Application form no later than **Wednesday, October 1st by 4:00 p.m.**

The online application form must be completed and submitted with the following required attachment uploaded:

- Attachment B: Budget Excel Workbook (in Excel format, not PDF) uploaded to online application form.

Please Note: The application and attachments are to be submitted electronically via the online application form. Emailed submissions will **NOT** be accepted.

For questions regarding this AGF, please email:

- **Sarah E. Cook, Program Coordinator at: sarah.e.cook@mass.gov**; and/or
- **Ira Berberaj, Program Coordinator at: ira.berberaj@mass.gov**

All application-related questions must be emailed and will be posted periodically for public viewing.

This AGF and all other required documents can also be found on the Cybersecurity Incident Response Planning and Tabletop Exercise Grant Opportunity page of our website.