

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



## **Municipal Local Cybersecurity Grant Program**

**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**

**February 9, 2024**

*Municipal Local Cybersecurity Grant Program (MLCGP)*

**Applications Due: March 8, 2024; 4:00 p.m.**

**Overview**

The Office of Grants and Research (OGR) will make available approximately **\$7,289,717** to units of local government through the federal State and Local Cybersecurity Grant Program (SLCGP) award to assist local communities in strengthening cybersecurity while reducing systemic cyber risk. To keep pace with today’s dynamic and increasingly sophisticated cyber threat environment, local governments and local public entities in Massachusetts must adopt key cybersecurity best practices, take decisive steps to modernize their approach to cybersecurity, and advance towards a Zero Trust Architecture. This competitive grant opportunity is being referred to as the “**Municipal Local Cybersecurity Grant Program**” (MLCGP) to avoid confusion with the application process. There is no local cost match for the MLCGP.

**Applicant Eligibility**

Only a Massachusetts local unit of government (e.g., municipalities, regional school districts, regional water authorities) are eligible to apply under this grant program. The **Municipal Chief Executive Officer** (Mayor, City Manager, Town Administrator, Executive Director) of the local unit of government applying for a grant award must sign the application when submitted. Only one (1) application per local unit of government is permitted for consideration of funding.

A municipality may submit a joint application that includes other municipalities in an effort to streamline the grant administrative process for itself and neighboring or nearby communities. Each separate municipality participating in a joint application will be eligible for up to the maximum award amount of \$100,000.00 individually and up to maximum of \$300,000.00 collectively. For example, if a joint application represents a total of three (3) towns and the maximum award amount for a local unit of government participating is \$100,000.00, the total maximum award amount that may be requested is \$300,000.00. A municipality will not be permitted to file a joint application if goods and services are not directly benefiting all listed partnering municipalities. No more than ten (10) municipalities may participate in a joint application.

Please note, if a municipality wishes to submit a joint application representing **greater than 3 municipalities**, the maximum amount of funding allowed to be requested may **NOT exceed \$300,000.00**. A municipality listed as a partner within a joint application submitted may NOT also submit an additional application as a primary applicant.

## Purpose

This grant opportunity is a competitive solicitation for local units of government within Massachusetts, interested in preventing, protecting against, mitigating, responding to, and recovering from cybersecurity threats and attacks. The purpose of funding under this AGF is to assist local units of government with improving cybersecurity by reducing susceptibility to cybersecurity threats, reducing cybersecurity vulnerabilities, and mitigating the consequences of a cybersecurity attacks by enhancing specific cybersecurity capabilities. Funding will be specifically used to acquire allowable equipment and services. Supplanting of funds is strictly prohibited. Funds for programs and services provided through this grant are intended to supplement, not supplant, other state or local funding.

## Key Dates

AGF POSTED	February 9, 2024
Application Assistance Webinar ( <b>Optional</b> )	February 16, 2024, at 11:00 a.m.  Please register for Municipal Local Cybersecurity Grant Program Applicant Information Session <a href="#">here</a> .  After registering, you will receive a confirmation email containing information about joining the webinar.  Brought to you by GoTo Webinar® Webinars Made Easy®
<b>Application Due Date</b>	<b>4:00 p.m. Friday, March 8, 2024</b>
Award Notification ( <i>anticipated</i> )	May 2024
Performance Period	May 2024-June 30, 2025

## Application Requirements

Under this solicitation, applicants must be a Massachusetts local unit of government. Only one (1) application per local unit of government will be permitted. The maximum amount of funding that may be requested by a unit of local government submitting an individual application is \$100,000.00. If a joint application is submitted, the maximum amount that may be requested is \$300,000.00 with the local units of government participating in the joint application each receiving no more than \$100,000.00. A local unit of government and/or its agencies may not submit or participate in more than one application.

Applicants must identify an allowable project for funding from the list of objectives below. In accordance with federal requirements, local jurisdictions or local public entities submitting subrecipient applications for the MLCGP must address at least one or more of the five (5) Project Objectives listed in the next section in their

proposed project(s) as specifically defined in the Massachusetts State and Local Cybersecurity Grant Program Plan (MA SLCGP Plan). The MA SLCGP Plan can be obtained by municipal and local public agency applicants by emailing [sarah.e.cook@mass.gov](mailto:sarah.e.cook@mass.gov). The release of the MA SLCGP Plan to state and local government applicants was approved by the MA SLCGP Planning Committee. The MA SLCGP Plan is not for public dissemination and is to be treated by applicants as For Official Use Only (FOUO) and will only be released by OGR to authorized state and local government applicants.

Applications proposing projects not identified as addressing a cybersecurity objective in this AGF will not be approved. Applications from a local unit of government must propose a project for funding from one of the following objectives:

### **Project Objectives**

This AGF provides five (5) Objectives from the MA SLCGP Plan that applicants must select from to identify an allowable project that assists a local community in achieving the purpose of the MLCGP. The objectives are within the MA SLCGP Plan’s goals to “Implement Cybersecurity Best Practices and Security Protections Commensurate with Risk” and “Create Cyber Workforce Plans that Develop and Train Employees Commensurate with Responsibility.” Only applications proposing a project from one of these five (5) Objectives will be given consideration based on their importance towards reducing and mitigating cyber risk.

### **Project Objectives:**

1. Migration of the local municipality or local public entity to the .gov internet domain.
2. Implementation of multi-factor authentication (MFA).
3. Cybersecurity awareness training –Municipalities with a .gov domain or a network email domain owned and managed by the local unit of government are eligible to apply.
4. Development of a written cybersecurity incident response plan for a local unit of government.
5. Tabletop exercises (TTX) involving cross-functional staff members, including senior leadership of the applicant to exercise, test, and refine written cyber incident response plans.

### **Application Priorities**

1. Include a detailed explanation of:
  - a. the intended uses of funds provided under the grant and
  - b. how the activities funded under the grant will meet the purpose;
  - c. If a joint application, letters of intent from the Chief Executive Officer from each joint applicant stating their commitment to participate in and comply with all

MLCGP requirements, a description of how the primary applicant will ensure that all jointly participating applicants will benefit, and information specifying what allowable program and services each participating local unit of government will receive.

2. Include an assurance that the applicant will maintain and report all data, records, and information (programmatic and financial) that OGR may reasonably require; in a joint application, the local unit of government that is the primary applicant will also maintain and report all data, records, and information (programmatic and financial) that OGR may reasonably require on behalf of it and all other joint applicants;
3. Include a certification within your application that:
  - a. the programs to be funded by the grant meet all the requirements of this AGF;
  - b. all the information contained in the application is true and correct; and
  - c. the applicant will comply with all provisions of this AGF and all other applicable State and Federal laws.

### **Maximum Award Amount**

No award made to a single unit of local government may exceed **\$100,000.00**. If a municipality wishes to submit a joint application that consists of one additional partner, the applicant may not request more than \$200,000.00 in funding. A joint application consisting of 3-10 municipalities will not be awarded more than \$300,000.00 in total funding.

### **Project Duration**

The period of performance for this grant is one year. Applicants must have their program completed by June 30, 2025. The anticipated funding cycle for projects will be **May 2024 through the end of June 2025**.

### **Funding Disbursement**

This is a cost reimbursement grant. Reimbursement requests must be submitted to OGR on a quarterly basis. Details about the reimbursement process will be provided upon award notification.

### **Subrecipient Requirements**

Subrecipients must abide by the federal grant requirements below as well as all OGR Subrecipient Grant Conditions to be provided at the time of contracting.

### **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:

- a. Be registered in [SAM.gov](https://sam.gov) before application submission;

- b. Provide a valid Unique Entity Identifier (UEI) in its application; and
- c. Continue to always maintain an active System for Award Management (SAM) registration with current information during the Federal Award process.

Note that 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.*

### **Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM)**

Applying for an award under this program is a multi-step process and requires time to complete. 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 unique entity identifier (UEI). The UEI number is issued by the SAM system. Requesting a UEI using [SAM.gov](https://sam.gov) is straightforward; the link can be found at <https://sam.gov/content/entity-registration>. Note that subrecipients do not need to have a valid UEI at the time of application but must have a valid UEI in order to receive a subaward.

### **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.

To register for the free grant required Cyber Hygiene Services, email: [vulnerability@cisa.dhs.gov](mailto: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). HSEEP guidance for exercise design, development, conduct, evaluation, and

improvement planning is located at <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>.

### **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](http://www.cisecurity.org).

### **Recommended Membership in the Multi State-Information Sharing and Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):**

Additionally, 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](http://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>.

### **Grants Management**

1. Submission of satisfactory and timely quarterly progress reports and quarterly financial reports with all required back-up documentation.
2. Cooperation during OGR monitoring endeavors, including site visits and desk reviews.

3. Supplanting of funds is strictly prohibited. Funds for programs and services provided through this grant are intended to supplement, not supplant, other state or local funding sources.
4. All costs paid with grant funds must be direct and specific to the execution of the MLCGP funded through the United States Department of Homeland Security (DHS) State and Local Cybersecurity Grant Program (SLCGP).
5. 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**

1. Subrecipients choosing to further subgrant all or any part of the award to an implementing agency or an independent contractor will enter into a written contract or memorandum of understanding (MOU) with the implementing agency or independent contractor. This written contract or MOU will include the provisions of the OGR standard subgrant conditions, and must, at a minimum explicitly outline the expected deliverables, timeframes/hours, and rates.
2. A copy of the contract or MOU must be submitted to OGR once an award is made.
3. Procurement of services, equipment, and supplies must follow M.G.L. Ch. 30B for local units of government and non-profit entities and Operational Services Division (OSD) Purchasing Guide for state agencies. Local units of government must ensure that subcontracts with private organizations have provisions ensuring any goods and services provided by the subcontractor are consistent with M.G.L. Ch. 30B procedures.

### **Other Requirements**

1. In addition to the requirements set forth above, subrecipients are required to agree to and abide by all state rules, regulations, and conditions pertaining to the receipt, administration, and management of grant funding.
2. OGR subgrant conditions must be signed and dated at the time an award is made.
3. All costs charged to this award covered by this AGF must comply with the federal Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200. This includes that costs must be incurred, and products and services must be delivered, within the period of performance of the award.



## **Equipment and Technology**

1. Equipment acquired with grant funds will be used and managed to ensure that the equipment is used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments.
2. All equipment must meet all applicable statutory, regulatory, and DHS standards to be eligible for purchasing using these funds.
3. In addition, recipients are responsible to obtain and maintain all necessary certifications and licenses for the requested equipment. Investments in emergency communications equipment must meet applicable SAFECOM Guidance recommendations. Such investments must be coordinated with the Statewide Interoperability Coordinator (SWIC) and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.
4. MLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing stand-alone warranty or extending an existing maintenance on an already-owned piece of equipment system, coverage purchase may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with MLCGP funds or for equipment dedicated for MLCGP related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.
5. Subrecipients are responsible for replacing or repairing the property that is willfully or negligently lost, stolen, damaged, or destroyed. Any loss, damage, or theft of the property must be investigated, fully documented, and made part of the official project records. A copy of the police report must be forwarded to OGR.

## **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. To report alleged waste, fraud, or abuse in 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 online at: [www.oig.dhs.gov/hotline](http://www.oig.dhs.gov/hotline).

## Evaluation Criteria

Proposals will be evaluated based on the Evaluation Criteria listed below. It is important that proposals clearly and completely address these requirements. The Attachment A Application and Attachment B (Excel) Budget Workbook must be completed and include the following:

1. **Applicant Information (10 points maximum): Full contact information is required for all applicants, whether individual or joint.**

2. **Needs Assessment (15):**

- Describe the municipality(s) and community(s) that will benefit from this award.
- Provide the 2020 U.S. Census residential population of the municipality(s) participating in the application and / or serviced by the local unit of government applicant or joint applicant (e.g., regional school district, regional water district, etc.).
- Describe your municipality(s) current unmet cybersecurity needs. Include detail about how grant funding will help address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of local governments.
- Describe related initiatives within your municipality (if applicable). If not applicable, please indicate this in your application.

It is important for applicants to address *all questions completely within this section. The narratives should be clearly written.*

3. **Project Description (25):**

Please use the space provided to:

- Describe the allowable project(s) with a detailed project scope that meets the criteria of the Municipal Local Cybersecurity Grant Program (MLCGP).
- Describe the expected outcomes within the performance period and how those outcomes will be measured.
- Provide a brief narrative identifying how the project(s) will be sustained by the municipality(s) or local unit of government, in the future.
- Briefly describe how this project(s) will be managed, including key roles and responsibilities, and identification of key personnel.
- Provide a usage plan for equipment and owners of the proposed assets to be procured (if applicable). If not applicable, please indicate this in your application.

In a joint application, the primary applicant must provide procurement services to all joint applicants partnering with them. The usage plan must include a description of the procurement process and, if applicable, tracking and ownership of all allowable goods and services to ensure compliance with all laws and requirements. This must include ensuring that any other joint applicants receive, track, and own, as applicable, the goods and services they are obtaining as described in the application.

It is important for applicants to address *all questions completely within this section. The narratives should be clearly written.*

In a joint application, the primary applicant must provide procurement services to all joint applicants partnering with them. The usage plan must include a description of the procurement process and, if applicable, tracking and ownership of all allowable goods and services to ensure compliance with all laws and requirements. This must include ensuring that any other joint applicants receive, track, and own, as applicable, the goods and services they are obtaining as described in the application.

It is important for applicants to address *all questions completely within this section. The narratives should be clearly written.*

4. **MLCGP Project Objectives (10 points maximum):** A detailed description of how the proposed project(s) supports the MLCGP Project Objectives. Please refer to the MA SLCGP Plan for details on meeting the allowable project objectives.
5. **Milestones (15 points maximum):** 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).
6. **Budget Narrative & Budget Details (25 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 cost category, by cost, and by description of expenditure. If a joint application, each local unit of government participating in it must be separately described by budget breakdown, cost category, cost, and description of expenditure.

**OGR will utilize the *Sub-Grantee Risk Assessment Form* through its review process to help identify if additional monitoring plan(s) 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 the appropriate applicant’s monitoring described in 2 CFR 200.331(b). If a joint application, each participating joint applicant must submit a Sub-Grantee Risk Assessment Form.

### **Additional Application Guidance**

To the extent applicable, follow the “Who, What, When, Where, Why, and How” approach.

- **Who** (specifically) will benefit from this proposal, and who will implement the project?
- **What** (specifically) is being proposed, and what will be the outcome? (Define the project and its scope.)
- **When** will the project begin and end?
- **Where** will any equipment be located and/or where will project activities be focused?
- **Why** is this project important? **How** was this determined? **How** will the project be implemented?

## Review Process

Please note that these questions above are provided as a general guide to assist applicants so that sufficient detail and specificity is included. For example, a proposal merely stating, “*Cybersecurity software will be procured,*” does not provide enough detail.

## Budget Section and Budget Excel Worksheet

This section should include costs that are reasonable and allowable under the MLCGP. Budgets should include both itemized and total costs. The information provided here must align with the Project Summary Section. It is incumbent on the applicant to verify allowable costs and the information prior to submitting the application. Applicants must also complete a Budget Excel Worksheet (refer to Attachment B). Please be sure to complete both Excel tabs (the Summary sheet and Detail worksheet) and submit with your application.

## Allowable Budget 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)

Definitions of each budget cost category are provided.

Allowable Budget Cost Categories	Definitions and Documentation Requirements
Consultants/Contract Costs	Consultant or Contractor fees associated with the equipment/technology purchased. For example, a consultant might be hired to install the technology.
Equipment/Technology Costs	Tangible non-expendable personal property having a useful life of more than one year; cost based on classification of equipment. Shipping and handling charges for equipment purchased should be placed in this cost category.
Other Costs	Supplies directly correlated to the equipment purchased. For example, ink or paper for a printer, batteries, etc.

## Unallowable Costs

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

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

This is a competitive grant and will be subject to a review process. All applications will be reviewed and scored by three (3) reviewers. The OGR Executive Director or his designee will present the award recommendations made by the reviewers to the Massachusetts State and Local Cybersecurity Grant Program Planning Committee.

In addition to scoring recommendations, when determining an award, other considerations, such as achieving geographic diversity, strategic priorities, past performance, and available funding can be factored into the decision process. Please note, federal guidelines require that rural areas receive at least 25% of the overall award's total funding. A rural area is defined in the federal requirements as an area encompassing a population of less than 50,000 people.

Applications from rural local jurisdictions and rural areas will receive priority consideration to meet this requirement. If additional funds become available, the OGR reserves the right to award additional applications considered worthy of funding.

### **Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services**

Subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act. This Act prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

### **Notification of Awards**

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.

### **Submission Process and Deadline**

Please review the following instructions carefully as there are two separate steps involved in submitting the Application, Budget and other documents.

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

*This AGF and all other required documents can also be found on our website:*  
<https://www.mass.gov/info-details/municipal-local-cybersecurity-grant-program>

**If you have any questions regarding this application, please reach out to:**

**Sarah E. Cook, Program Coordinator**  
[Sarah.e.cook@mass.gov](mailto:Sarah.e.cook@mass.gov)

## **Hard Copy and Electronic Submission**

### **Step 1: Electronic Submission**

Submit your [Online Application form](#) no later than **Friday, March 8<sup>th</sup> at 4:00 p.m.**

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

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

Submission of the online form alone will not be accepted as an application submission.

### **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:

- The complete, printed, signed application, Attachment A
- Attachment B: Budget Excel Workbook (Summary and Detail)

Online Applications must be submitted no later than **4:00 p.m. on Friday, March 8, 2024**, and hard copy of the application and documents must be postmarked on or before this date and mailed to:

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