

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



**2026 Counter-Unmanned Aircraft Systems Grant
Program**

**Maura T. Healey
Governor**

**Kimberley Driscoll
Lieutenant Governor**

**Gina K. Kwon
Secretary**

**Kevin J. Stanton
Executive Director**

**Commonwealth of Massachusetts
Executive Office of Public Safety and Security
Office of Grants and Research**

**2026 Counter-Unmanned Aircraft Systems Grant Program
Availability of Grant Funds**

Applications due November 26, 2025, by 4:00pm

Introduction

The Office of Grants and Research (OGR), a state agency that is part of the Executive Office of Public Safety and Security (EOPSS), supports public safety through the dissemination of state and federal grant funds focused on criminal justice, traffic safety, law enforcement and homeland security initiatives. OGR is the State Administering Agency (SAA) for federal funds received from the Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA), Department of Justice (DOJ) and the National Highway Traffic Safety Administration (NHTSA). As the SAA for DHS/FEMA funding, OGR is responsible for managing and administering the [Counter-Unmanned Aircraft Systems Grant Program](#) (CUASGP).

CUASGP Overview and Purpose

The CUASGP, was established under Section 90005(a) of the [One Big Beautiful Bill Act](#), 2025 (Pub. L. No. 119-21), in direct response to growing national security concerns surrounding the unlawful or nefarious use of unmanned aircraft systems (UAS). OGR anticipates OGR anticipates a minimum of **\$3.325 million but could receive a much higher award if interest and need exists from our local and state public safety organizations**. Potential additional funds could be made available based on the risks and needs presented.

The program's priorities are shaped by Executive Order 14305, "Restoring American Airspace Sovereignty," and recommendations from the White House FIFA World Cup Task Force and subject matter experts from the field.

The CUASGP provides funding to enhance state and local capabilities to detect, identify, track, or monitor unmanned aircraft systems (as defined in 49 U.S.C. § 44801), consistent with Titles 18 and 49 of the U.S.C. This funding supports U.S. state, local, tribal, and territorial governments in combatting the unlawful use of unmanned aircraft systems that pose a threat to the safety and security of the American people, communities, and institutions.

Administration of Federal Funds

Per federal rules and regulations, the SAA is the only entity eligible to submit a CUASGP application to DHS/FEMA for these funds. Per 6 U.S.C. 609(a)(12), the states may retain up to 3% of awarded funds to pay expenses directly related to the administration of the grant (i.e., Management and Administration (M&A) costs). SAAs must pass through at least 97% of funds to eligible subrecipients. The only exception is that the SAA may retain a portion of funds with appropriate justification, to make equipment purchases, or support activities at the state level that benefit state law enforcement agencies or address other statewide needs for this technology. The amount of funds that can be retained by the SAA under this exception cannot exceed 20% of the total awarded funding.

Key Dates

Application Due Date	11/26/2025 by 4:00pm
OGR Award Announcements	Tentative: January 2026
Grant Period of Performance	Approved Start Date-September 30, 2028

Eligible Applicants

For the purpose of this Availability of Grant Funds (AGF), **eligible applicants may include state, local, tribal, and territorial government entities, including city and county public safety agencies, law enforcement, fire services, emergency medical services, emergency management, state college campus police departments, and other qualifying public safety organizations.** An applicant must be a Massachusetts recognized tribal organization, municipality, or state agency in order to be eligible to apply.

CUASGP can be used for the purchasing of:

- Unmanned aircraft system (UAS) detection;
- Identifying, monitoring, tracking, and mitigation (DIMIT-M) technologies to support public safety officials in the protection of the public and critical infrastructure from nefarious or unlawful use of UAS; and
- Mitigation technologies (please note this will be limited to select jurisdictions).

Funds for C-UAS mitigation capabilities (e.g., kinetic or non-kinetic capabilities used to disable, destroy, or seize control of during flight) may only be authorized for law enforcement or correctional agencies which have personnel trained at or are scheduled to be trained at the FBI's National C-UAS Training Center on C-UAS mitigation operations. Applicants must ensure that all mitigation operations are conducted in compliance with applicable laws and regulations.

Per DHS, applicants should not have foreign nationals or noncitizens included. If an applicant has foreign nationals, they must be properly vetted and must adhere to all government statutes, policies, and procedures including “staff American, stay in America” and security requirements. Please note this in your application for DHS/FEMA review.

Funding Availability

OGR anticipates that a minimum of **\$3.325 million will be made available for state agencies** to competitively solicit. However, the Commonwealth could receive a much higher federal award if there is great interest and need reflected in our application to DHS/FEMA. OGR is strongly encouraging all eligible applicant types to submit if need exists.

Funding Priorities

The CUASGP’s primary objective is to ensure all eligible agencies and public safety entities have the resources, training, and operational capacity to detect, track, identify, and – where authorized – mitigate UAS threats. It is anticipated that 80% of these funds will be utilized for purchase of C-UAS equipment and/or services. The remaining 20% shall be utilized for training personnel in the operation of C-UAS technology. The program’s goals are to:

1. Strengthen national preparedness by equipping SLTT agencies with C-UAS capabilities.
2. Protect critical infrastructure, mass gatherings, and sensitive government operations from UAS threats.
3. Support the deployment of fixed or portable systems for UAS detection, tracking, identification, and – where authorized – mitigation, consistent with applicable laws.

Allowable Costs

Allowable costs for this program generally fall into five main categories: planning, organization, equipment, training, and exercises (POETE). By funding activities across the POETE framework, the CUASGP can ensure a comprehensive approach to building and sustaining capabilities for the detection, tracking, identifying, and mitigation (DTIM) technologies to support public safety officials in the protection of the public and critical infrastructure from nefarious or unlawful use of UAS. Please see **Appendix A** of this AGF for allowable activity examples. **Please note grant awardees will be required to provide a detailed cost breakdown at the time of contracting.** Grant funds must be used to supplement existing funds and not replace (supplant) funds that have been appropriated for the same purpose.

Additional examples of the POETE framework applied to the C-UAS Grant Program include, but are not limited to⁴:

Purpose	Type	Examples
Planning		
Plan Development	Operations	- Implementation Plan - Standard Operating Procedures
Organization		
System Deployment	Personnel	- Program Management - Operational Overtime
Equipment		
Detection	Sensors Cameras	- Radar systems - Electro Optical and Infrared Cameras - Passive Acoustic Systems
Tracking	Remote ID Systems Broadcast Beacon Receivers	- Remote ID Receivers - GPS-Based Tracking Systems - ADS-B (Automatic Dependent Surveillance-Broadcast) Receivers - Wi-Fi and Bluetooth Receivers Radios
Identification	UAS Identification Systems Operator Identification Systems UAS Forensics Tools	- Remote ID Decoders - AI-Based Video Analytics - RF Signal Triangulation - Geolocation Systems
Mitigation	Radio Frequency Systems Kinetic Systems	- Fixed or mounted jammers - GPS or Command and control Spoofers - Net deployment systems - Intercept (a.k.a. kamikaze) UAS
Deployment, Operation & Maintenance	Vehicles Services/Subscriptions Equipment Operations and Maintenance	- Trailers - Generators - Point to Point links - Mesh Networking
Training		
Detection, Tracking, Identification	Vendor-based	Training
Mitigation	FBI's NCUTC	- Training - Certification
Detection, Tracking, Identification, Mitigation	Internally Executed Vendor-supported	- Seminar - Workshop - Tabletop Exercise - Drill - Functional Exercise - Full-Scale Exercise

⁴ This list is not exhaustive, all C-UAS costs must be in certified as compliant with Title 18 by the Department of Justice.

All C-UAS costs must have a demonstrated nexus to achieving target capabilities related to preventing, preparing for, protecting against, and responding to acts of terrorism in accordance with 6 U.S.C. 609(a) and 605(a). C-UAS funds may also be used in a manner than enhances preparedness for disasters unrelated to acts of terrorism, if such use assists such governments in achieving target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism, pursuant to 6

U.S.C. 609(c). Additional details on the technology or services covered by this grant program can be found in the [NOFO](#) pages 44-46.

Per FEMA, applicants using funds for personnel costs may be required to submit short biographies and resumes. OGR will contact awardees if this is needed at the time of contracting.

C-UAS technologies exist to support public safety officials in protection of public and critical infrastructure from nefarious or unlawful use of UAS. These technologies employ a variety of sensors and processes which detect, track, identify, and mitigate a threat UAS. Detection, tracking, and identification of UAS may be provided by a third-party as a service, generally for wide-area UAS airspace awareness. To facilitate protection of a fixed site or public event, different detection, tracking, and identification equipment is used, which is generally owned and paired with mitigation technologies. Proper training, maintenance, and use of these technologies ensure safe employment in the National Airspace and efficacy in protecting the public.

All agencies and personnel operating mitigation technologies purchased or supported with CUASGP funds must:

1. Have personnel trained at, or scheduled to be trained at, the FBI's National Counter-UAS Training Center (FBI NCUTC). FEMA will verify registration with the FBI to ensure compliance with this requirement.
2. Include proof of registration and, where applicable, certification with their grant application and maintain this documentation for compliance purposes. Equipment not in regular use, or used for unauthorized purposes, may be subject to recovery, and the recipient may be required to return grant funds. Documentation of usage and deployment must be maintained and submitted in performance progress reports.

Management and Administration

Allowable management and administration (M&A) costs are necessary direct costs incurred in direct support of the federal award or as a consequence of it, such as travel, meeting-related expenses, and salaries of full/ part-time staff in direct support of the program. As such, M&A costs can be itemized in financial reports. If an outside consultant or contractor is used for grant writing or grant management, additional federal requirements may apply. **Subrecipients may use up to 3% of their CUASGP funds for M&A purposes.**

Operational Overtime

Overtime hours being charged against the award are only eligible for reimbursement for actual hours worked regardless of department policy or union contract rules. For example, an officer working one hour of overtime on a federally funded project

awarded by OGR is prohibited from charging the grant award for four hours of overtime due to a union contract. A department that must allow for this will need to cover the remaining three hours of overtime from their own state or local budget. Departments found violating this policy will be subject to immediate termination of a grant award and must return all misspent funds to OGR. CUASGP-funded projects that include operational overtime require additional documentation, including specifying which types of overtime are eligible. Aside from the National Terrorism Advisory System alerts, which do not require pre-approval, operational overtime must be preapproved before an event. CUASGP funds may not be used to support the hiring of sworn public safety officers for purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities ([6 U.S.C. § 609\(b\)\(1\)\(A\)](#)).

Federal Procurement Standards

Spending under CUASGP must comply with all applicable federal and state procurement standards described in 2 CFR 200.317 through 200.326 and provided by OGR via a Subgrant Conditions Form at the time of contracting. Subrecipients must also follow their own documented procurement procedures which reflect applicable federal and state rules and regulations.

Following federal requirements does not exempt subrecipients from state or local requirements. In some instances, state and/or local procurement requirements may be more stringent than the federal procurement regulations. Subrecipients must ensure any actions taken satisfy federal and state requirements.

Additionally, OGR reserves the right to suspend or terminate a contract for non-compliance with the applicable procurement regulations. OGR is required to have policies and procedures for integrity of funds. Subrecipients will be subject to additional reporting requirements and further budget breakdowns. Please contact OGR staff for guidance when necessary. For more terms and conditions, please see attached [DHS Standard Terms and Conditions | Homeland Security](#).

Mitigation Technologies

Law enforcement officers may use force against a drone when they reasonably believe it is necessary to protect themselves or others from an imminent threat of death or serious physical injury. This authority is grounded in the Fourth Amendment and Supreme Court precedents such as *Tennessee v. Garner*, (471 U.S. 1 (1985)) and *Graham v. Connor*, (490 U.S. 386 (1989)). These principles extend to drones used as weapons or otherwise presenting an imminent threat. However, Congress, recognizing the need for broader authority to address a wider variety of public safety situations, provided reliefs from prosecution under a variety of Federal laws that could be implicated when

countering UAS threats. Congress did not extend those reliefs to SLTT entities. To enable SLTT personnel to operate the full range of mitigation technologies (e.g., kinetic or non-kinetic capabilities used to disable, destroy, or seize control of during flight), the Department of Justice acting through the FBI shall deputize SLTT law enforcement or correctional facility officers in the FBI Joint Terrorism Task Forces (JTTF). To employ mitigation technologies, these JTTF members must attend and complete the training course at FBI's NCUTC. SLTT JTTF may only conduct C-UAS mitigation operations within their federal capacity, unless acting when they reasonably believe it necessary to protect themselves or others from imminent death or serious injury.

Detection, Tracking, and Identification Technologies or Services

Under U.S. law, any entity – whether an individual, private organization, or government agency at the federal, state, local, tribal or territorial level – may lawfully detect, track, and identify an UAS so long as the activity is limited to point-of-fact observable information or communications “readily accessible to the public.” Courts have consistently recognized that there is no reasonable expectation of privacy in information exposed to public view or broadcast into the public domain (*Katz v. United States*, 389 U.S. 347 (1967); *California v. Ciraolo*, 476 U.S. 207 (1986)).

The Wiretap Act (18 U.S.C. § 2511(2)(g)(i)) expressly permits interception of radio communications “readily accessible to the general public,” a category encompassing Remote ID broadcasts required by the FAA (14 C.F.R. Part 89). Additionally, the Wiretap Act expressly permits the interception of radio communications of aeronautical communications (18 U.S.C. § 2511(2)(g)(ii)(IV)). For a UAS, 47 CFR § 88.5 defines the aeronautical communications of “control and non-payload communications” as any transmission that is sent between the unmanned aircraft component and the UAS ground station of the UAS and that supports the safety or regularity of the unmanned aircraft's flight.

Detection technologies – such as visual observation, radar (active or passive), EO/IR sensors, passive radio frequency detection, or acoustic detection – do not implicate the Wiretap Act or Pen Register/Trap and Trace statute (18 U.S.C. §§ 3121–3127). These systems detect physical reflections or the presence of emissions, not communications. As a matter of law and physics, they cannot constitute unlawful interception. Thus, visual observation, radar returns, optical tracking, acoustic signatures, Remote ID data, and aeronautical communications of “control and non-payload communications” fall outside wiretap restrictions.

The sharing or retention of aeronautical control and non-payload communications and other information “readily accessible to the general public” is not restricted by 6 U.S.C. § 124n, 50 U.S.C. § 2661 or 10 U.S.C. § 130i. Those statutes provide relief only for

otherwise unlawful acts, not for data already public, Remote ID, visual point-of-fact, radar, and acoustic detections that are publicly accessible and may be freely shared or retained.

Radio frequency (RF) detection technologies that electronically intercept radio communications “readily accessible to the general public” or that are “aeronautical control and non-payload communications” are not subject to wiretap or pen registry/trap restrictions. Since the UAS telemetry and control data do not concern traditional user-initiated content, or addressing, these detection technologies do not constitute a pen trap or register. RF interception technologies that capture user-generated “payload” data or content, such as video feeds, are specifically immunized under 6 U.S.C. § 124n.

Acquisition and Use of Technology to Mitigate UAS (Counter-UAS)

The malicious use of UAS poses safety and security risks to soft targets and crowded places. When considering various C-UAS equipment or services, SLTT public safety entities may engage the DHS Science and Technology Directorate (S&T) National Urban Security Technology Laboratory (NUSTL) for further guidance through NUSTL@hq.dhs.gov or through the Federal Bureau of Investigation National Counter Unmanned Aircraft Systems Training Center (FBI NCUTC). NUSTL has knowledge products and technical advisory services available to public safety entities. All purchases of mitigation equipment must be coordinated with the FBI NCUTC. These advisory services will be provided for informational purposes only. Guidance received is not binding and lacks the force and effect of law, unless expressly authorized by statute or expressly incorporated into a contract, grant, or cooperative agreement.

It is strongly recommended that, prior to the testing, acquisition, installation, or use of UAS detection and/or mitigation systems, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. Entities should conduct their own legal and technical analysis of each UAS detection and/or mitigation system and should not rely solely on vendors’ representations of the systems’ legality or functionality. Please also see the DHS press release on this topic for further information: [Interagency Issues Advisory on Use of Technology to Detect and Mitigate Unmanned Aircraft Systems | Homeland Security](#).

Unallowable Cost

Projects are ineligible if they do not align with the CUASGP purpose and fail to demonstrate a clear nexus to preventing, preparing for, protecting against, or responding to acts of terrorism. Additionally, projects that include activities not permitted under the CUASGP guidance or that do not meet the criteria for allowable

costs will not be funded. Please see **Appendix B** for detailed breakdown of unallowable costs.

Recipients may not use federal funds or any cost share funds for the following activities:

1. Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).
2. Lobbying or other prohibited activities under 18 U.S.C § 1913 or 2 C.F.R. § 200.450.
3. Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).
4. Any activities inconsistent with Federal laws and any laws or regulations applicable to their jurisdiction. Such activities must also be consistent with the First and Fourth Amendments to the Constitution.
5. Not all equipment that is considered controlled equipment is allowed under the CUASGP. As noted in Section B of FEMA Policy 207-22-0002, [Prohibited or Controlled Equipment Under FEMA Awards](#), certain equipment is prohibited and is not allowable under CUASGP.

Application Instructions

To provide OGR the best opportunity to fairly evaluate all requests for funding, applicants are encouraged to be clear and concise in their proposals. All applicants will be required to submit an Online Application and all required attachments to apply for funding.

Applicant Information

- Contact Information: Provide applicant identification and legal/ tax information, and contact information for senior agency official, grant contact, and fiscal manager
- Program Summary: provide a summary of the activities to be funded (250 characters)

Applicant Role and Experience

- Description of your agency's background and expertise in providing safety and security for large events
- Explanation of previous and/or current involvement in strategic security-related planning with EOPSS (if applicable)
- Explanation of anticipated role in providing safety and security for World Cup Boston 2026

Completing the Investment Justification (IJ) Form

The IJ should demonstrate how the proposed project aligns with the CUASGP objectives and enhances the applicant's capabilities to detect, track, and respond to threats posed by UAS. The IJ includes a specific section for each of the allowable activities listed in the AGF. Please complete all sections. **It is extremely important that applicants provide as much detail as possible (including itemized budget costs) so that the SAA and DHS/FEMA have enough information to possibly support applicant requests.** If you are not requesting funds in a cost category, indicate "Not Applicable." Please do not leave the field blank.

Additionally, if your project proposal includes M&A costs, please specify these costs under the applicable category. For example, if M&A is to be requested in relation to planning costs, please include the details of your M&A request under the planning category.

When completing the IJ, an applicant must complete the following sections for each allowable activity for which funds are being requested. Again, if an activity area is not applicable, please indicate so by writing "N/A":

- **Project Description:** Describe the planned activities, services, or equipment purchases that will be funded by the grant and provide a clear overview of the project's purpose, scope, and intended outcomes.
- **Capability Gap:** Explain how planned activities will address or have addressed gaps in public safety and security. Highlight current gaps in UAS detection, tracking, or response capabilities. Describe the specific threats, vulnerabilities, or risks posed by UAS in your jurisdiction.
- **Project Objectives:** Specify how requested funding will address program objectives for the relevant allowable activity. Describe how the project will enhance public safety, protect critical infrastructure, and mitigate UAS-related threats.
- **Subrecipient Impact** (if applicable): Describe how local/tribal governments and public safety entities will assist in described activities.
- **Performance Goals:** Specify how requested funding will address performance goals listed in the NOFO for the relevant allowable activity. Identify specific, measurable outcomes that will be used to evaluate the project's success.
- **Budget and Timeline:** Provide a detailed budget breakdown and timeline for project completion and implementation of costs, including key milestones.

Completing the Budget Narrative

The Budget Narrative should outline the budget requested and itemize the expenses by cost category as described in this application. For each cost category that has an associated funding request, please provide a description and justification of that cost category. Please be advised that this AGF attempts to highlight allowable and unallowable costs, as well as pertinent state and federal rules and regulations, but it is the responsibility of the applicant to utilize the links embedded throughout this AGF for further guidance and assistance. Even costs deemed allowable in this document could be overruled by DHS/FEMA. **Please note OGR will require awardees to submit a detailed budget breakdown at contracting.**

Application Review Process

All requests for funding will undergo a screening process to assist in determining awards.

A peer review process will be conducted by the SAA. Reviewers are responsible for ensuring all stated AGF rules and regulations are adhered to, such as application completeness, answering questions posed, ensuring projects have a homeland security nexus, etc. Preference for funding will be given to applicants proposing to utilize these funds to protect the Boston 2026 World Cup event.

DHS/FEMA has provided the following scoring mechanism which can also be found on pages 27-31 of the [NOFO](#), that states must utilize when making award recommendations.

Category	Description	Points
Mitigation	Proposal includes kinetic or radio frequency intercept capabilities, such as spoofers, jammers, net systems or “kamikaze” drones and training (only FBI NCUTC training and equipment consistent with the technological capabilities of the equipment used at the FBI’s NCUTC).	0-30
Radar	Proposal includes radar with a mission-appropriate use case and basic siting/coverage concept.	0-2
Electro-Optical/Infrared	Proposal includes EO/IR with day/night operations and a simple integration/cueing concept.	0-2
Passive RF (non-content)	Proposal includes passive RF that inspects physical waveforms only (no content/payload reading) and names at least one DF method (TDOA, FDOA, POA, or AOA).	0-2
Remote ID/broadcast beacon receivers	Proposal includes Remote ID compliant with ASTM F3411-22a or vendor broadcast intended for government receipt without intercepting protected communications.	0-2
Detect-Track-Identify chain	Proposal clearly describes how it will detect, track, and identify UAS (mitigation may be described only if properly authorized, but is not required to earn these points).	0-2
Deployment/connectivity equipment plan	Proposal includes needed deployment and connectivity elements (e.g., networking gear, point-to-point or mesh links, vehicles/trailers/generators) to support the sensors.	0-2

Category	Description	Points
Wide Area SaaS	Proposal enables lawful data sharing with DHS, DOJ, DOE, and DOD C-UAS operating entities (e.g., data outputs/viewer/cloud access) and, if using DaaS, aligns with the described service model and local records/retention rules. Additionally, proposal includes a service which has applied for or received FAA approval as a provider of unmanned traffic management (UTM) data through the FAA's Near-Term Approval Process (NTAP) for UTM Services program and covers a major metropolitan area of at least 100 sq. miles.	0-2
Training and operator readiness	Proposal provides a role-based training plan mapped to the proposed systems (operators/maintainers/supervisors), covers safety and applicable legal constraints for signal handling, and includes an exercise or validation component. If mitigation is proposed, operator qualifications are included only when authorization is documented.	0-2
Capability Type (enhancement/maintenance)	New capability: Introduces a function not currently present in the jurisdiction (e.g., first-time passive RF DF, first Remote ID deployment) with a clear deployment plan (worth 2 pts) Enhancement/maintenance: Measurably expands coverage, improves detection/tracking quality, adds DF nodes, replaces end-of-life units, or sustains critical capability with a clear integration and sustainment plan. (worth 1 pt)	1-2
Timely Implementation	Proposal includes a realistic schedule and contracting/readiness steps to fully implement (procure, install, train, and operationalize) within 6 months of award (worth 2 pts) Proposal includes a realistic schedule and contracting/readiness steps to fully implement (procure, install, train, and operationalize) within 12 months of award (worth 1 pt)	1-2
NSSE, SEAR 1or 2 Events	Proposal specifies support in cities hosting an event of National significance, including FIFA World Cup and national America 250 events with an NSSE, SEAR 1 or 2 level designation (applicant must specify name, date, and city of event and verify project implementation prior to the event).	0-50
		TOTAL: 0-100

The SAA will then embed the outcome of this process into our state application for DHS/FEMA consideration. DHS/FEMA will review the state application (which will include all requests received regardless of the SAA funding recommendation) and make final decisions for all subawards, including award amounts.

Application Submission and Deadline

All applications, including required attachments, must be submitted using the [Online Application Form](#).

*This AGF, other required documents, as well as additional informative resources can also be found on the C-UAS [Grant Program Funding Opportunity](#) page of OGR's website.

During the application period, OGR Special Projects Manager Sarah Malloy will be available to provide specific guidance to individual applicants as needed and may be reached by email at .

All applicants must complete and submit the following items with their application:

- Screen shot print out from System for Award Management (SAM) that includes agency name, Unique Entity Identifier (UEI).
- OGR Sub-Grantee Risk Assessment form.
- Investment Justification (IJ) form
- Indirect Cost (IDC) Rate Agreement, if included in budget
- Fringe Rate Agreement, if included in budget

Unique Entity Identifier (UEI)

All applicants for this award must have a valid UEI (formerly DUNS number). Information on how to request a UEI Number from SAM.gov is located here: [Entity Registration | SAM.gov](#).

OGR Sub-Grantee Risk Assessment

Federal regulations contained in Title 2 CFR §200.331 require that OGR evaluate each applicant's subrecipient's risk of non-compliance with Federal statutes, regulations, and the terms and conditions of the sub-award for purposes of determining the appropriate subrecipient monitoring. **In order to comply, the OGR Sub-Grantee Risk Assessment Form is included within this AGF. All applicants are required to complete and submit the OGR Risk Assessment Form along with their application.** OGR will utilize the Risk Assessment Form through its review process to help us determine appropriate monitoring plans for sub-recipients. **Please note that the OGR Sub-Grantee Risk Assessment Form is used to evaluate compliance risk, not risks associated with threats or hazards.** 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.

Environmental Planning and Historic Preservation (EHP) Compliance

All proposed construction and renovation activities must undergo an EHP review, including approval of the review from FEMA, prior to undertaking any action related to the project. Failure of a grant recipient to meet these requirements may jeopardize Federal funding. Please be advised certain equipment and technology may also require EHP review. See the [Preparedness Grants Manual](#) Section 4.5, which is incorporated by reference into this AGF, for information on EHP compliance.

Disclaimer

Please be advised that OGR reserves the right to amend this opportunity and revise language included in this AGF if funding rules and regulations are amended by FEMA. OGR reserves the right to cancel this opportunity if the Commonwealth is not awarded these federal funds or unable to comply with federal grant administrative regulations being required to accept this award. It is the responsibility of applicants to check our website regularly for any updates or revisions being made to this opportunity. All OGR award recommendations are also subject to FEMA approval.

All applications, including required attachments, must be submitted using the [Online Application Form](#) on or before **November 26, 2025, by 4:00pm**. Emailed submissions will NOT be accepted. Please notify OGR immediately if you are unable to utilize the online application. All questions should be directed to Special Projects Manager Sarah Malloy at Sarah.A.Malloy@mass.gov.

Appendix A: Allowable Activity Examples

Purpose	Type	Examples
Planning		
Plan Development	Operations	• Implementation Plan • Standard Operating Procedures
Organization		
System Deployment	Personnel	• Program Management • Operational Overtime
Equipment		
Detection	Sensors Cameras	• Radar systems • Electro Optical and Infrared Cameras • Passive Acoustic Systems
Tracking	Remote ID Systems Broadcast Beacon Receivers	• Remote ID Receivers • GPS-Based Tracking Systems • ADS-B (Automatic Dependent Surveillance-Broadcast) Receivers • Wi-Fi and Bluetooth Receivers Radios
Identification	UAS Identification Systems Operator Identification Systems UAS Forensics Tools	• Remote ID Decoders • AI-Based Video Analytics • RF Signal Triangulation • Geolocation Systems
Mitigation	Radio Frequency Systems Kinetic Systems	• Fixed or mounted jammers • GPS or Command and control Spoofers • Net deployment systems • Intercept (a.k.a. kamikaze) UAS
Deployment, Operation & Maintenance	Vehicles Services/Subscriptions Equipment Operations and Maintenance	• Trailers • Generators • Point to Point links • Mesh Networking
Training		
Detection, Tracking, Identification	Vendor-based	• Training
Mitigation	FBI's NCUTC	• Training • Certification
Detection, Tracking, Identification, Mitigation	Internally Executed Vendor-supported	• Seminar • Workshop • Tabletop Exercise • Drill • Functional Exercise • Full-Scale Exercise

Appendix B: Unallowable Costs Detailed

Program-Specific Unallowable Costs	Description
Program-Specific-Weapons and Accessories	Per FEMA policy and published in Information Bulletin No. 530, the purchase of weapons and weapons accessories, including ammunition, is not allowed with C-UAS Grant Program funds. Grant funds may not be used for the purchase of the following equipment: firearms; ammunition; grenade launchers; bayonets; or weaponized aircraft, vessels, or vehicles of any kind with weapons installed. (For the purposes of this NOFO, “weaponized aircraft” refers to any aircraft, manned or unmanned, that is equipped with, or designed to deliver, weapons or munitions. Non-weaponized aircraft and UAS (drones) used for monitoring, surveillance, or data collection are not prohibited, unless otherwise specified. Requests for technologies with dual-use or mitigation functions that may fall into a gray area should be submitted to FEMA for pre-approval and justification.)
Program-Specific-General Use Facility Expenditures	• General-use facility expenditures, to include, but not limited to ordinary facility maintenance, contracts for maintenance, and specifically backup or emergency generators; • General vehicle maintenance, service contracts, or warranties. This is different from maintenance and sustainment costs that are allowable, but only for projects funded under a grant award. For projects or equipment not funded by the grant award, general maintenance, service contracts, and warranties are not allowable; • Expenditures for items such as general-use software (word processing, spreadsheet, graphics, etc.); general-use computers and related equipment (other than for allowable M&A activities, or otherwise associated preparedness or response functions); general-use vehicles, licensing fees, recurring operating costs (e.g., cell phone services, maintenance contracts);
Organizational Operating Expenses	• Personnel costs including, but not limited to, overtime and backfill (except as detailed within this NOFO). Personnel costs are only allowable when directly related to the purpose of the NOFO and approved projects. • Activities not directly related to the completion or implementation of C-UAS Grant Program-funded projects and activities; • Other indirect costs (meaning property purchase, depreciation, or amortization expenses);
	• Initiatives in which federal agencies are the beneficiary or that enhance federal property; • Initiatives which study technology development; • Proof-of-concept initiatives; • Initiatives that duplicate capabilities being provided by the Federal Government; and • Other items not in accordance with the Authorized Equipment List, Information Bulletin No. 530, or not previously listed as allowable costs. • Per 6 USC 609(b)(1), grant funds will be used to supplement existing funds and will not replace (supplant) funds that have been appropriated for the same purpose. Applicants or recipients may be required to supply documentation certifying that a reduction in non- federal resources occurred for reasons other than the receipt or expected receipt of federal funds.