FY 2026 Counter-Unmanned Aircraft Systems (C-UAS) Grant Program

Notice of Funding Opportunity (NOFO)

Grant Issued By:

U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Grant Programs Directorate (GPD)

Grant Issued Through:

Missouri Department of Public Safety (DPS), Office of Homeland Security (OHS)

Assistance Listing:

97.161

Funding Opportunity Title

FY 2026 Counter-Unmanned Aircraft Systems (C-UAS) Grant Program

Introduction

The Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) is pleased to announce the funding opportunity for the FY 2026 Counter-Unmanned Aircraft Systems (C-UAS) Grant Program. This state administered, but federally funded program, is made available through the Grants Programs Directorate (GPD) within the Federal Emergency Management Agency (FEMA).

Program Description

The C-UAS Grant Program was established in Fiscal Year 2026 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).

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. These priorities specifically address the elevated security demands of high-profile events, including the FIFA World Cup 2026 and national America 250 celebrations.

The C-UAS Grant Program provides resources to state, local, tribal, and territorial (SLTT) agencies, first responders, and public safety entities to detect, track, and identify (DTI) UAS

threats, ensuring the safety of the public, critical infrastructure, and sensitive government operations.

Goals and Objectives

The C-UAS Grant Program's primary objective is to ensure SLTT agencies and public safety entities have the resources, training, and operational capacity to detect, track, and identify UAS threats.

The program's goals are to:

1. Strengthen national preparedness by equipping SLTT agencies with C-UAS Grant Program's 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, and identification consistent with applicable laws.

FEMA created the C-UAS Grant Program to ensure that SLTT agencies receive funds to purchase DTI equipment or services for the detection, tracking, and identification, of UA and UAS signals consistent with the legal authorities of those SLTTs. Under this grant program, SLTT entities and first responder and/or public safety entities may use federal funds through grant programs to purchase fixed or portable systems that can detect, track, and identify UAS threats consistent with applicable laws.

Period of Performance: 19 months

Projected Period of Performance Start Date: March 1, 2026

Projected Period of Performance End Date: September 30, 2027

Eligible Applicants:

Local government entities, including city and county agencies, law enforcement, fire services, emergency medical services, emergency management, and other qualifying public safety organizations.

DPS GRANTS – STATE REQUIREMENTS

To be eligible for grant funding through the Missouri Department of Public Safety (DPS), agencies must be compliant with the requirements listed below (as applicable) at the time of application and if awarded funding, must maintain compliance throughout the grant period of performance.

LAW ENFORCEMENT REQUIREMENTS

These requirements below apply only to law enforcement agencies.

Each law enforcement agency shall certify compliance with these requirements below when applying for grants administered by the DPS.

Section 590.650 RSMo – Vehicle Stops Report

Pursuant to Section 590.650.3 RSMo, each law enforcement agency shall compile the data described in subsection 2 for the calendar year into a report to the attorney general and each law enforcement agency shall submit the report to the attorney general no later than March first of the following calendar year.

NOTE: Failure to submit the Vehicle Stops (Racial Profiling) Report will result in the automatic denial of the application.

Section 590.700 RSMo – Written Policy on Recording of Custodial Interrogations

Pursuant to Section 590.700.4 RSMo, each law enforcement agency shall adopt a written policy to record custodial interrogations of persons suspected of committing or attempting to commit felony crimes as outlined in subsection 2.

Section 43.544 RSMo – Written Policy on Forwarding Intoxication-Related Traffic Offenses

Pursuant to Section 43.544.1 RSMo, each law enforcement agency shall adopt a policy requiring arrest information for all intoxication-related traffic offenses be forwarded to the central repository as required by Section 43.503 RSMo.

Section 590.1265 RSMo – Police Use of Force Transparency Act of 2021

Pursuant to Section 590.1265 RSMo, each law enforcement agency shall report data submitted under subsection 3 of this section to the department of public safety.

For purposes of grant eligibility, law enforcement agencies will be considered non-compliant if they have not submitted Use of Force reports for three or more months in the previous 12 months.

NOTE: Show Me Crime Reporting provides a no cost option for agencies to comply with Section 590.1265 RSMo. Agencies not currently compliant with Section 590.1265 RSMo will not be eligible to apply until they have registered with Show Me Crime Reporting and have begun submitting Use of Force reports.
https://showmecrime.mo.gov/CrimeReporting/ForcePage.html

Section 43.505 RSMo – Uniform Crime Reporting (UCR)

Pursuant to Section RSMo 43.505.3, each law enforcement agency in the state shall: (1) Submit crime incident reports to the department of public safety on forms or in the format prescribed by the department; and (2) Submit any other crime incident information which may be required by the department of public safety.

Agencies not compliant at the time of application will be ineligible for funding unless the grant allows funds to be utilized to assist the agency to become compliant.

For purposes of grant eligibility, law enforcement agencies will be considered non-compliant if they have not submitted MIBRS reports for three or more months in the previous 12 months.

NOTE: Show Me Crime Reporting provides a no cost option for agencies to comply with Section 43.505 RSMo. Agencies not currently compliant with Section 43.505 RSMo will not be eligible to apply until they have registered with Show Me Crime Reporting and have begun submitting MIBRS reports.
https://showmecrime.mo.gov/CrimeReporting/MIBRSRegistration.html

Section 590.030 RSMo – Rap Back Program Participation

Pursuant to Section 590.030 RSMo, all law enforcement agencies shall enroll in the state and federal Rap Back programs on or before January 1, 2022 and continue to remain enrolled. The law enforcement agency shall take all necessary steps to maintain officer enrollment for all officers commissioned with that agency in the Rap Back programs. An officer shall submit to being fingerprinted at any law enforcement agency upon commissioning and for as long as the officer is commissioned with that agency.

FIRE AGENCY REQUIREMENT

This requirement applies only to fire agencies.

Section 320.271 RSMo – Fire Department Registration

Pursuant to Section 320.271 RSMo, all fire protection districts, fire departments, and all volunteer fire protection associations as defined in section 320.300 shall complete and file with the state fire marshal within sixty days after January 1, 2008, and annually thereafter, a fire department registration form provided by the state fire marshal.

EMS REQUIREMENTS

These requirements apply only to EMS agencies.

Section 190.105 RSMo – Ambulance License

Pursuant to Section 190.105 RSMo, no person, either as owner, agency or otherwise, shall furnish, operate, conduct, maintain, advertise, or otherwise be engaged in or profess to be engaged in the business or service of the transportation of patients by ambulance in the air, upon the streets, alleys, or any public way or place of the state of Missouri unless such person holds a currently valid license from the department for an ambulance service pursuant to the provisions of sections 190.001 RSMo to 190.245.

NOTE: If the applicant agency is an ambulance service, a copy of the license certificate as required by section 190.105 RSMo MUST be submitted in the Named Attachments component of the application.

Section 190.133 RSMo – Emergency Medical Response Agency License

Pursuant to Section 190.133(4) RSMo, no person or entity shall hold itself out as an emergency medical response agency that provides advanced life support or provide the services of an emergency medical response agency that provides advanced life support unless such person or entity is licensed by the state of Missouri Department of Health and Senior Services.

NOTE: If the applicant agency is an emergency medical response agency, a copy of the license certificate as required by section 190.133(4) RSMo MUST be submitted in the Named Attachments component of the application.

Ineligible Applicants

- State agencies
- Nonprofit organizations
- For-profit organizations

Application and Submission Information

1. **Key Dates and Times**

   a. Application Start Date: November 17, 2025

   b. Application Submission Deadline: November 24, 2025, 4:00 pm CST

2. **Agreeing to Terms and Conditions of the Award**

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

3. **Application Maximum Award: There is no maximum award. This grant program is competitive through DHS/FEMA among seven states (California, Georgia, Missouri, Kansas, Massachusetts, Washington, and Pennsylvania) with $105,050,000 in funding available.**

Applications will only be accepted through the Missouri Department of Public Safety (DPS) online WebGrants System.

As part of the FY 2026 C-UAS application, each eligible applicant must complete all application forms and provide all required documents:

1. **Contact Information**

2. **DPS Grants State Requirements**

3. **Project Package**

4. **Budget**

5. **Named Attachments**
    a. **Audit/Financial Statement (REQUIRED)**
    b. **Investment Justification (REQUIRED)**
        i. **Refer to Appendix B for instructions**
    c. **Quote (REQUIRED)**
    d. **Other Supporting Information (up to 5 attachments)**

General Funding Requirements

Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules and regulations, policies, this NOFO, and the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period.

Subrecipients 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
2. Lobbying or other prohibited activities
3. Prosecuting claims against the federal government or any other government entity
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.

Prohibition on Covered Equipment or Services

Subrecipients and their contractors or subcontractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which restrict the purchase of covered telecommunications and surveillance equipment and services. Please see 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200, and FEMA Policy #405-143-1 – Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services for more information.

Application Criteria

Applicants must clearly describe the operational need for UAS detection capabilities in their jurisdiction, including specific threats, vulnerabilities, or gaps that the project will address. The Investment Justification must outline the proposed project and implementation plan, detailing the activities to be undertaken, the timeline for completion, and how the project will enhance UAS detection, tracking, and response capabilities. Additionally, applicants must include a detailed budget that breaks down costs by category (e.g., Planning, Organization, Equipment, Training, and Exercises) and provides a justification for each expense. All submissions must adhere to the requirements outlined in the Notice of Funding Opportunity (NOFO) and comply with applicable federal laws and regulations.

Proposals will be considered based on the project's adherence to eligible costs outlined below. Partial funding may be approved to remove ineligible costs that are not specified or deemed unallowable.

Funding Categories and Technologies

C-UAS Grant Program 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, and identify 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. Proper training, maintenance and use of these technologies ensure safe employment in the National Airspace and efficacy in protecting the public. Funding under this grant program may be used for but not limited to:

1. **Planning**

    - Developing or updating UAS-specific response plans that integrate detection systems into existing emergency operations plans (EOPs) or incident command systems.
    - Conducting risk assessments to identify high-priority areas for UAS detection, such as critical infrastructure, public events, or disaster-prone areas.
    - Developing standard operating procedures (SOPs) for responding to unauthorized or malicious UAS activity.
    - Coordinating with federal agencies (e.g., FAA, DHS) to ensure compliance with federal laws and regulations governing UAS detection and mitigation.
    - Establishing information-sharing protocols with fusion centers, law enforcement, and other stakeholders to disseminate UAS-related threat intelligence.
    - Planning for the integration of UAS detection systems with existing public safety technologies, such as Geospatial Information Systems (GIS) platforms or computer-aided dispatch (CAD) systems.

2. **Organization**

    - Salaries for personnel supporting C-UAS operations.
    - Developing or updating UAS-specific response plans that integrate detection systems into existing EOPs or incident command systems.
    - Conducting risk assessments to identify high-priority areas for UAS detection, such as critical infrastructure, public events, or disaster-prone areas.
    - Developing SOPs for responding to unauthorized or malicious UAS activity.

3. **Equipment**

    - For detection, tracking, and identification:

    - Radar (active and passive)
    - Electro Optical and Infrared Cameras
    - Radio Frequency Detection Systems
    - Acoustic Systems
    - Remote ID and similar broadcast beacon receivers
    - Integrated multi-sensor systems include all or some of the above
    - Senior fusion software and hardware
    - Networking communications
- Third Party Data Service Providers.
- Acquiring sensor fusion software to integrate data from multiple detection systems into a common operational picture (COP).
- Procuring portable/mobile UAS detection systems for use during temporary events or in remote areas.
- Investing in UAS software-as-a-service (SaaS) subscription models to access cutting-edge technology without the need for large upfront investments, including but not limited to surveillance as a service and data as a service.
- Purchasing mounts, masts, power supplies, and networking equipment to support the deployment of UAS detection systems.
- Procuring calibration tools and spares to ensure the ongoing functionality of detection equipment.

4. Training and travel

- Training programs for C-UAS systems.
- Attendance at FBI NCUTC.
- Necessary related travel costs for C-UAS personnel adhering to federal U.S General Services Administration standards and policy.
- Providing hands-on training for first responders on the operation of specific UAS detection systems.
- Conducting train-the-trainer programs to build local capacity for ongoing training efforts.
- Providing scenario-based training to prepare responders for real-world UAS threats, such as swarming drones or UAS equipped with payloads.
- Training personnel on the interpretation of UAS detection data and the integration of this data into decision-making processes.

5. Exercising

- Conducting tabletop exercises (TTXs) to simulate UAS-related incidents and test response plans, SOPs, and coordination protocols.
- Organizing functional exercises (FXs) to test the operation of UAS detection systems and the integration of these systems with other public safety technologies.
- Running full-scale exercises (FSEs) to simulate large-scale UAS threats, such as unauthorized UAS activity at a public event or near critical infrastructure.

- Including multi-jurisdictional exercises to test coordination between state, local, tribal, and federal agencies, as well as private sector partners.
- Conducting after-action reviews (AARs) to identify lessons learned and areas for improvement following exercises.
- Incorporating UAS detection scenarios into broader homeland security exercises, such as those focused on terrorism or disaster response.

See Appendix A: Allowable Activities for additional information on these funding categories and technologies.

Unallowable Costs

- 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 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 purpose 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.*)
- 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, general-use vehicles, licensing fees, recurring operating costs (e.g., cell phone services, maintenance contracts)
- Organizational operating expenses
- Personnel costs, to include, 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
- Other items not in accordance with the AEL, in accordance with 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.

Legal Considerations

6 U.S.C. § 124n provided authorization to engage in C-UAS activities notwithstanding other federal laws, such as Air Piracy (49 U.S.C. § 46502), Aircraft Sabotage (18 U.S.C. § 32), Computer Fraud and Abuse Act (18 U.S.C. § 1030), Interference with a satellite (18 U.S.C. § 1367), Pen Registry/Trap (18 U.S.C. §§ 3121–3127), and the Wiretap Act (18 U.S.C. § 2511). That statutory authorization is in addition to the pre-existing authority of law enforcement, including SLTT law enforcement, to act 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 unmanned aircraft system (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 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 are publicly accessible and may be freely shared or retained.

Radio frequency (RF) detection technologies which electronically intercept radio communications "readily accessible to the general public" or 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. Radio frequency (RF) interception technologies which capture user-generated "payload" data or content, such as video feeds, are specifically immunized under 6 U.S.C. § 124n.

Participate in Data Sharing

DHS, DOJ, Department of Energy (DOE), or Department of War (DOW) C-UAS operating entities may request data from grant subrecipients for C-UAS operations that include but are not limited to public safety and national security. As allowed by applicable jurisdictional records retention policies, data sharing restrictions, and information law, the grant subrecipient shall enter a vendor contract which enables efficient and reasonable data sharing with DHS, DOJ, DOE, DOW C-UAS operating entities. Such data sharing mechanisms may include but are not limited to data output file transfer, limited viewer access, or shared cloud access.

As allowed by applicable local jurisdictional records retention policies and information law, the grant subrecipient may identify other SLTT public safety entities with mutual interest in UAS detection and tracking. After identifying SLTT public safety partners, the grant subrecipient may enter a vendor contract which allows for identified partner public safety entities to access data as a user.

Administrative and National Policy Requirements

Presidential Executive Orders

Subrecipients must comply with the requirements of Presidential Executive Orders related to grants (also known as federal assistance and financial assistance), the full text of which are incorporated by reference.

In accordance with Executive Order 14305, Restoring American Airspace Sovereignty (June 6, 2025), and to the extent allowed by law, eligible state and local grant subrecipients under this NOFO are permitted to purchase unmanned aircraft systems, otherwise known as, drones, or equipment or services for the detection, tracking, or identification of drones and drone signals, consistent with the legal authorities of state and local agencies. Subrecipients must comply with all applicable federal, state, and local laws and regulations, and adhere to any statutory requirements on the use of federal funds for such unmanned aircraft systems, equipment, or services.

DHS Standard Terms and Conditions

A subrecipient under this funding opportunity must comply with the DHS Standard Terms and Conditions in effect of the date of the federal award. The DHS Standard Terms and Conditions are available at DHS Standard Terms and Conditions.

Environmental Planning and Historic Preservation (EHP) Compliance

FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities, grants, and programs funded by FEMA, comply with federal Environmental Planning and Historic Preservation (EHP) laws, Executive Orders (EO), regulations, and policies.

Subrecipients proposing projects with the potential to impact the environment or cultural resources, such as the modification or renovation of existing buildings, structures and facilities, and/or new construction and/or replacement of buildings, structures, and facilities must participate in the FEMA EHP review process. This includes conducting early engagement to help identify EHP resources, such as threatened or endangered species, historic properties, or communities with environmental concerns; submitting a detailed project description with supporting documentation to determine whether the proposed project has the potential to impact EHP resources; and identifying mitigation measures and/or alternative courses of action that may lessen impacts to those resources.

FEMA is sometimes required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not in compliance with applicable EHP laws, Executive Orders, regulations, and policies. FEMA may recommend mitigation measures and/or alternative courses of action to lessen impacts to EHP resources and bring the project into EHP compliance.

EHP guidance is found at Environmental Planning and Historic Preservation. The site contains links to documents identifying agency EHP responsibilities and program requirements, such as implementation of the National Environmental Policy Act and other EHP laws, regulations, and Executive Orders. DHS and FEMA EHP policy is also fund in the EHP Directive and Instruction.

All FEMA actions, including grants, must comply with National Flood Insurance Program (NFIP) criteria or any more restrictive federal, state, or local floodplain management standards or building code (44 C.F.R. § 9.11(d)(6)). For actions located within or that may affect a floodplain or wetland, the following alternatives must be considered: a) no action; b) alternative locations; and c) alternative actions, including alternative actions that use natural features or nature-based solutions. Where possible, natural features and nature-based solutions shall be used. If not practicable as an alternative on their own, natural features, and nature-based solutions may be incorporated into actions as minimization measures.

The GPD EHP screening form is located on FEMA's website. The form should be submitted to the DPS/OHS.

Monitoring and Oversight

Per 2 C.F.R. § 200.337, DHS and its authorized representatives have the right of access to any records of the subrecipient pertinent to a Federal award to perform audits, site visits, and any

other official use. The right also includes timely and reasonable access to the subrecipient's personnel for the purpose of interview and discussion related to such documents or the Federal award in general. Pursuant to this right and per 2 C.F.R. § 200.329, DHS may con project accomplishments and management control systems as well as provide any required technical assistance. Subrecipients must respond in a timely and accurate manner to DHS/DPS/OHS requests for information relating to a federal award.

Build America, Buy America Act

Subrecipients must comply with FEMA's implementation requirements of the Build America, Buy America Act (BABAA), which was enacted as part of the Infrastructure Investment and Jobs Act §§ 70901-70927, Pub. L. No. 117-58 (2021); and Executive Order 14005, Ensuring the Future is Made in All of America by All of America's Workers. See also 2 C.F.R. Part 184, Buy America Preferences for Infrastructure Projects and Office of Management and Budget (OMB) Memorandum M-24-02, Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure.

None of the funds provided under this program may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.

To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to implement FEMA's Build America, Buy America requirements, please see Programs and Definitions: Build America, Buy America Act.

a. Waivers

When necessary, subrecipients may apply for, and FEMA may grant, a waiver from these requirements.

A waiver of the domestic content procurement preference may be granted by the agency awarding official if FEMA determines that:

- Applying the domestic content procurement preference would be inconsistent with the public interest
- The types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactorily quality

- The inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25%

The process for requesting a waiver from the Buy America preference requirements can be found on FEMA's website at: "Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure.

Contact Information:

Additional information and resources can be located on the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) website: Missouri Department of Public Safety, Office of Homeland Security - Grants Section.

Applications must be submitted online at Missouri Department of Public Safety's WebGrants System.

Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS):

Chelsey Call
Grants Supervisor
(573) 526-9203
Chelsey.Call@dps.mo.gov

Joni McCarter
Program Manager
(573) 526-9020
Joni.McCarter@dps.mo.gov

Kelsey Saunders
Grant Support Specialist
(573) 522-6125
Kelsey.Saunders@dps.mo.gov

Appendix A: Allowable Activities

To maximize the impact of the grant program, POETE activities should be integrated into a cohesive strategy. For example:

- Planning: Develop a UAS response plan
- Organization: Cover program management costs and operational overtime
- Equipment: Procure/deploy DTI systems
- Training: Train personnel on system operation and response protocols
- Exercises: Test the system and response plan in a simulated incident

By funding activities across the POETE framework, the C-UAS Grant Program can ensure a comprehensive approach to building and sustaining capabilities for the detection, tracking, and identifying (DTI) technologies to support public safety officials in the protection of the public and critical infrastructure from nefarious or unlawful use of UAS. Additional examples of the POETE framework applied to the C-UAS Grant Program include, but are not limited to:

Purpose	Type	Examples
Planning		
Plan Development	Operations	• Implementation Plan • Standard Operating Procedures
Organization		
System Development	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
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
Exercises		
Detection, Tracking, Identification	Internally Executed	• Seminar • Workshop • Tabletop Exercise • Drill • Functional Exercise • Full-Scale Exercise
	Vendor-supported	

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

Additional Details on the Technology or Services Covered by this Grant Program

Subrecipients must purchase technologies that comply to all applicable federal statutes as well as the laws of jurisdictions where the equipment will be located and operated. It is strongly recommended that, prior to the testing, acquisition, installation, or use of UAS detection systems, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. This is particularly important because potential legal prohibitions are not based on broad classifications of systems (e.g., active versus passive), but instead are based on the functionality of each system and the specific ways in which a system operates and is used. A thorough understanding of both applicable law and the systems' functionality will ensure important technologies designed to protect public safety, by detecting UAS threats, are used effectively, responsibly, and legally. 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, and identify 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. Proper training, maintenance and use of these technologies ensure safe employment in the National Airspace and efficacy in protecting the public. Funding under this grant program may be used for:

1. Active Radar

Description: Radars generally operate by transmitting a radio signal of known frequency and power in a focused direction and then detecting the reflected signal that is bounced back from the target.

2. Passive Radar – Radio Frequency (RF)

Description: Passive radar systems used to track drones detect and track targets by analyzing reflections of existing electromagnetic and radio frequency signals, such as commercial broadcast, cellular, or navigation transmissions, rather than emitting their own signals. By comparing direct-path and reflected signals, passive radar determines the range, velocity, and trajectory of a drone. These systems are well-suited for urban and sensitive environments due to their non-emissive nature.

They are effective against small drones, especially when integrated with data fusion platforms, providing continuous monitoring without contributing to the electromagnetic spectrum or requiring dedicated transmissions.

3. Electro Optical and Infrared Cameras

Description: EO/IR sensors are digital video cameras that collect environmental information in the visible and infrared light spectrum.

4. RF Direction Finding

Description: Radio frequency (RF) directional finders used to detect and track drones passively scan the electromagnetic spectrum for the presence of drone emissions, such as command-and- control (C2) links and telemetry signals. These systems identify signal sources without intercepting or decoding protected content. Directional antennas and triangulation techniques determine bearing and geolocation of active drone and controller signals. RF finders support situational awareness by alerting operators to unauthorized drone activity and cueing other sensors. When integrated into multi-sensor C-UAS systems, they enhance threat detection and classification without capturing the content of private communications.

Specifications: Systems that rely solely on inspecting the physical waveform of the RF Spectrum to identify and classify UAS-related signals based on their unique characteristics and/or direction-finding techniques are permitted. The following are common passive RF system direction-finding techniques which do not require additional statutory authority, and are therefore permissible for purchase through this grant program:

- Time Difference of Arrival (TDOA)
- Frequency Difference of Arrival (FDOA)
- Power of Arrival (POA)
- Angle of Arrival (AOA)

5. Passive Acoustic Systems

Description: Acoustic sensors are passive and use high sensitivity microphone arrays coupled with audio analysis applications to detect, track and identify sounds produced by UAV motors and propellers.

6. Remote ID and similar broadcast beacon receivers

Description: Remote ID is the ability of a UAS in flight to provide identification and location information that can be received by other parties or is generally accessible to the general public through a broadcast signal. Some UAS manufacturers may also voluntarily broadcast UAS telemetry using protocols not compliant with ASTM F3411-22a but with the express intent of it being received by government agencies. *See* Remote Identification of Drones | Federal Aviation Administration for more information on Remote ID and associated FAA requirements.

7. Constraints – Interception of payload content

The grant program may not be used to purchase DTI systems which also gather UAS "payload data", which is any data that is not the aeronautical communications of "control and non-payload communications" (47 CFR § 88.5) of a UAS 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 UA's flight.

8. Third Party Data Service Providers

Vendors that deliver UAS detection data by one of the above means using equipment owned by the service provider typically employ a business model where detection hardware, software, and supporting infrastructure is set up in a geographical location and access to data is sold to various authorized users. As such, this grant may be used to fund third party data purchases from data as a service (DaaS) providers to manage, analyze, and utilize data outputs from the purchased system(s). The most comprehensive systems include built-in FAA-approved B4UFLY and LAANC tracking. This grant program provides scoring preference for services that have received or have applied for FAA approval as a UTM data provider.

9. Equipment for deployment, operation, and maintenance

This grant may be used to purchase other equipment required to deploy, operate, and maintain the aforementioned sensors, such as:

- Vehicles, trailers, generators, etc. required to transport and deploy sensors
- Services, subscriptions, software licenses
- Equipment required to connect sensors, to include traditional networking equipment, as well as tactical systems such as Point to Point links and mesh networking.
- Operations and maintenance

10. Training and Exercises

This grant may be used to fund training (including related travel expenses) of grant subrecipient agency personnel to operate and maintain the purchased equipment, as well as exercises to test the capacity of grant subrecipient agencies to successfully employ the acquired capabilities.

Appendix B: Investment Justification

Investment Justification (IJ) Framework

The IJ should demonstrate how the proposed project aligns with the **C-UAS Grant Program's objectives** and enhances the applicant's capabilities to detect, track, and respond to threats posed by unmanned aircraft systems (UAS). Applicants are encouraged to structure their IJ using the **POETE (Planning, Organization, Equipment, Training, and Exercises)** framework to ensure their projects address all necessary aspects of capability development.

a. *Investment Justification Components*

1. Project Description

- **What to Include:**
  - Describe the planned activities, services, or equipment purchases that will be funded by the grant.
  - Provide a clear overview of the project's purpose, scope, and intended outcomes.
- **POETE Connection:**
  - Break down the project into relevant POETE categories. For example:
    - **Planning:** Developing a UAS response plan to integrate detection systems into existing emergency operations plans.
    - **Organization:** Establishing a regional UAS task force to oversee detection and response efforts.
    - **Equipment:** Procuring radar-based UAS detection systems and sensor fusion software.
    - **Training:** Conducting FBI-certified training for first responders on UAS detection and response protocols.
    - **Exercises:** Organizing a full-scale exercise to test the effectiveness of the detection system and response plan.

2. Capability Gap

- **What to Include:**
  - Explain how the planned activities will address or have addressed gaps in public safety and security.
  - Describe the specific threats, vulnerabilities, or risks posed by UAS in the applicant's jurisdiction.
  - Highlight current gaps in UAS detection, tracking, or response capabilities.
- **POETE Connection:**
  - Link the identified capability gaps to the POETE framework. For example:
    - "Our jurisdiction lacks the **Equipment** to detect unauthorized UAS activity near critical infrastructure, as well as the **Training** to ensure first responders can effectively operate detection systems."

3. Project Objectives

- **What to Include:**
  - Specify how the requested funding will address the objectives listed in Appendix A of the NOFO for the relevant allowable activity.
  - Describe how the project will enhance public safety and protect critical infrastructure from UAS-related threats.
- **POETE Connection:**
  - Connect the project objectives to POETE activities. For example:
    - "The objective of this project is to deploy UAS detection systems (**Equipment**) and develop a comprehensive response plan (**Planning**) to enhance our jurisdiction's ability to detect and respond to unauthorized UAS activity."

4. Subrecipient Impact – <u>This section is not applicable and does not need to be completed.</u>

5. Performance Goals

- **What to Include:**
  - Specify how the requested funding will address the performance goals listed in Appendix A of the NOFO for the relevant allowable activity.
  - Identify specific, measurable outcomes that will be used to evaluate the project's success.
- **POETE Connection:**
  - Tie performance goals to POETE activities. For example:
    - "Performance goals include the deployment of two UAS detection systems (**Equipment**), the training of 50 first responders on UAS detection protocols (**Training**), and the completion of one multi-agency tabletop exercise (**Exercises**)."

6. Budget and Timeline

- **What to Include:**
  - Provide a detailed budget breakdown for project costs, including labor, materials, and equipment.
  - Include timelines for project completion and implementation, with key milestones clearly identified.
- **POETE Connection:**
  - Categorize costs under POETE. For example:
    - **Planning:** $10,000 for consultant services to develop a UAS response plan.
    - **Equipment:** $150,000 for radar-based UAS detection systems.
    - **Training:** $25,000 for training on UAS detection and response.
    - **Exercises:** $15,000 for a full-scale exercise to test the system and response plan.

b. ***Additional Guidance for Completing the IJ***

- **Use Data to Support the Need:** Include data, risk assessments, or real-world examples to substantiate the operational need for UAS detection capabilities.
- **Focus on Impact:** Emphasize how the project will enhance public safety, protect critical infrastructure, and address UAS-related threats.
- **Be Specific and Measurable:** Avoid vague statements. Provide concrete details about the project's scope, activities, and expected outcomes.

By following this framework and guidance, applicants can ensure their Investment Justification is comprehensive, well-structured, and clearly aligned with the C-UAS Grant Program's objectives and the POETE framework. This will help streamline the application review process and ensure that funding is awarded to projects that effectively enhance UAS DTI capabilities.