# Request for Proposal (RFP)

# Remote Surveillance System Design for Military Installations

Issue Date: October 12, 2022

# 1. Introduction

US Ignite, Inc. (US Ignite) is seeking proposals from technology partners to design a Remote Surveillance System for Military Installations as part of the Smart Installation and Community Dashboard (SICD) Program in support of the U.S. Army Garrison Fort Benning (FBGA). The Project includes a total of four Phases.

**Phase 1 - Remote Surveillance System Design**
Phase 2 - Installation
Phase 3 - Operations
Phase 4 - Project Completion

The scope of this RFP and contract award is for Phase 1 - Remote Surveillance System Design. The Final Design Proposal due at the end of the Phase 1 contract must meet the System Capability Requirements shown in Appendix A.

The overall objective of this pilot project is to quickly deploy a self-contained, temporary or semi-permanent, intelligent video surveillance system that edge-processes data from optical and thermal cameras to monitor remote locations on the installation to detect the presence of unauthorized soldiers, civilians and vehicles in real time. The system must include its own power and communications and be connected and integrated into the SICD to provide alerts to a number of directorates on FBGA to monitor and respond to the incident as needed. The system will record and retain the surveillance video and provide a user interface to manage the collected information for review and use in investigations.

US Ignite will evaluate and award contracts to one or more Proposers. The selected Proposer(s) must conduct a comprehensive site survey of the pilot deployment area at FBGA within 30 days of the contract award. Information gathered from the site visit and discussions with the project partners will be used to complete the Phase 1 deliverables, which includes preparing and presenting a Final Design Proposal. **The contract term for Phase 1 is expected to begin late November and end February 1, 2023. The award(s) available for Phase 1 is up to $25,000 available through a firm fixed price contract with US Ignite.**

US Ignite may select a Final Design Proposal. **The Proposer that may be selected will be awarded a new contract for project Phases 2 through 4, for completion by December 2023.** If the pilot deployment is successful in Phase 3, additional Remote Surveillance Systems may be procured and installed in other locations on FBGA.

The selected Proposer is expected to work collaboratively with the project partners that include FBGA, the U.S. Army Engineer Research and Development Center (ERDC), Columbus State University (CSU) and US Ignite through the duration of the SICD program.

# 2. US Ignite, Fort Benning and the Program Overview

## 2.1 US Ignite Overview

US Ignite is a national nonprofit, a 501(c)(3), that is accelerating the smart city movement – and creating

value for an entire ecosystem – by guiding communities into the connected future, creating a path for private sector growth, and advancing technology research that's at the heart of smart city development.

Why is this important? Because local governments need to improve the quality of life and ensure economic development in their communities, particularly during a time of rapid technological change. Businesses recognize the importance of the emerging market around smart communities and need to find commercial strategies that are repeatable, scalable, and sustainable. And foundations and federal agencies need to channel their institutional aims into efforts ranging from cutting-edge research to practical economic development initiatives that deliver measurable benefits.

As a trusted partner, US Ignite brings this entire smart city ecosystem together, successfully pairing financial investment with technical and organizational expertise. Through the public-private partnership programs we run, US Ignite is a catalyst for communications network advancement, and for innovation in smart city services that are powered by a new generation of technologies. You can read more about US Ignite's programs on its website.

## 2.2 Fort Benning Overview

Fort Benning is a U.S. Army base located south of Columbus, Georgia, and is home for the Maneuver Center of Excellence and its mission is to train and equip combat–ready Soldiers and Leaders. The base supports a population of almost 70,000 Soldiers and civilians in providing some of the military's most prestigious and rigorous leadership schools and functional training courses.

Fort Benning Facts:

- Military assigned to Fort Benning - 27,436
- 14,146 soldier and their families live off-base
- Fort Benning covers 284 square miles
- Fort Benning is the fifth largest military base

## 2.3 Fort Benning Smart Base Program Overview

The 2020 Army Installation Strategy (AIS) identifies a key feature of the operational environment as the accelerating rate of technological change. Future Soldiers will expect installations to modernize at pace with civilian sector smart cities initiatives. The challenge for the Department of Defense and the Army is establishing the necessary conditions to ensure safe, secure, and connected data-driven decisions for reducing costs and improving the environment, quality of life, security, and mission readiness.

FBGA has a broad interest in understanding automated systems in order to plan for a range of areas related to modernization, readiness, and quality of life. Efforts within this scope of work are sponsored by the Assistant Secretary of the Army (Acquisition, Logistics and Technology) with congressional appropriations entitled Smart Installation and Community Dashboard (SICD). SICD is managed by USACE-ERDC, and leverages support from the Assistant Secretary of the Army (Installations, Energy, and Environment) and their Installations of the Future program. The expected outcome of this research program is the development and demonstration of a smart installation and community pilot system for Fort Benning. This project will incorporate smart and automated technologies coupled with data analytics, data fusion, and artificial intelligence to provide faster awareness and decision options for Fort Benning staff with a framework that can be scalable to other installations.

## 2.4 Remote Surveillance Pilot Project Overview

FBGA is a large Army base that includes heavily wooded areas and a porous boundary that is challenging to patrol and secure. To protect and improve the safety of military personnel, DoD civilians, and family members who train, work, and live on the installation the Project will select, install, and operationalize an intelligent remote surveillance system at a pilot location. The Final Design Proposal selected and installed will identify, capture, and analyze threats to public safety and automatically alert FBGA stakeholders so the appropriate level of response can be activated.

Working with the project partners, the selected Proposer's remote surveillance system will be integrated with the SICD to provide a common operating picture for the FBGA leadership. After deployment, the system will be operated to verify the approach and allow for updates and functional refinements. If successful in the pilot location, the selected Proposer's solution may be scaled to additional locations on FBGA.

# 3. Scope of Services - Phase 1 Remote Surveillance System Pilot Project Design

This section describes the Scope of Services for Phase 1 - Remote Surveillance System Design, requested in this RFP.

## 3.1 Conduct Site Visit and Complete Trip Report

The selected Proposer(s) must conduct a site visit to FBGA to tour and inspect the area selected for the remote surveillance system pilot. US Ignite and FBGA will host the selected Proposer(s) and facilitate discussions to address any questions regarding the system requirements. The site visit will be completed in one day at the installation. A Trip Report capturing the findings from the visit must be provided to US Ignite within two weeks after the trip.

Additional locations may be toured during the site visit to include areas where the system could be scaled if the pilot proves successful.

## 3.2 Prepare Final Design Proposal

The selected Proposers must submit a comprehensive Final Design Proposal detailing how the proposed solution meets the project objectives. This Final Design Proposal must be informed by the lessons learned during the site visit, along with design discussions conducted with owners for systems to be integrated with as described in Appendix A.

Project partners to coordinate design decisions include:

1. US Ignite, the system integrator for the SICD cloud platform
2. US Army system owners for the Garrison Common Operating Picture (COP) hosted within a Microsoft Azure Government Cloud tenant
3. Front-end development team that has developed HMI wireframes and mock clickables, and is available as a resource for front-end development
4. Information system engineering support services vendor available as a networking, security, and system integration resource

5. Academic partner developing soldier, civilian, animal, and other object detection algorithms to be deployed onto the successful proposer's system

The Final Design Proposal must include the following elements:

1. Introduction with Executive Summary
2. Table of Contents
3. Project Objective
4. Proposed Solution Description
5. Process/Approach, Project Management Plan
6. System Capabilities - As compared to those listed in Appendix A
7. Statement of Work - Expected tasks and deliverables to be completed per Appendix B
8. Schedule - Include duration of tasks and major milestones through completion of the project
9. Bill of Materials, Equipment Specification Sheets, Installation Drawings
10. Engineering Drawings - System Architecture, Data Flow Diagrams, Security Architecture, Network Architecture
11. Cost - Format will be provided
12. Description of team assigned to Project and their roles and responsibilities
13. Proposer's experience with similar projects, sites and/or customers
14. Small Business Concerns

### 3.3 Present Final Design Presentation

The selected Proposers will present the Final Design Proposal in a presentation to US Ignite, FBGA and ERDC.

## 4. Deliverables and Project Timeline - Phase 1

**Table 1 - Target Schedule and Deliverables**

| Deliverable | Target Suspense | Content |
|---|---|---|
| Phase 1 Contract Award | 11/28/2022 | US Ignite awards Phase 1 contract to select Proposers |
| FBGA Site Visit Completed | 12/28/2022 | Proposer completes site survey of pilot deployment area at FBGA |
| Trip Report | 1/11/2023 | Site visit trip report completed and submitted |
| Final Design Proposal | 2/1/2023 | Final written proposal completed and submitted |
| Final Proposal Presentation | 2/1/2023 | Final presentation delivered to project partners |

# 5. Information for Proposers

## 5.1 Solicitation Timeline

**Table 2 -Solicitation Timeline**

| Deadline | Date |
|---|---|
| RFP Release | 10/12/2022 |
| Questions Due | 10/24/2022 |
| US Ignite Responses to Questions | 10/27/2022 |
| Proposals Due | 11/9/2022 |
| Contract Execution (Beginning of PoP) | 11/28/2022 |
| End of PoP | 2/1/2023 |

## 5.2 Questions and Answers

All clarification questions must be submitted by October 24, 2022, no later than 8:00 PM Eastern Daylight Time (EDT). Questions should be submitted in the following format:

- Section Number
- Paragraph Number
- Text of passage being questioned
- Question

All requests, questions, or other communications about this RFP shall be made in writing to sayed.elhamz@us-ignite.org . Communications made to other US Ignite personnel or attempts to ask questions by phone or in person will not be allowed or recognized as valid and may disqualify the supplier. Suppliers should only rely on written statements issued by the RFP coordinator. US Ignite will endeavor to respond to all parties no later than October 27, 2022 8:00 PM EDT.

## 5.3 Proposals to the RFP for Phase 1

All RFP proposals must be submitted by November 9, 2022 no later than 8:00 PM EDT via email to sayed.elhamz@us-ignite.org.

RFP Proposals must include:

5.3.1 Cover Page

Include primary contact information, including name, title, phone number, email, and organization name,

address, and DUNS number.

5.3.2 Remote Monitoring System Proposal
Write up on the approach that would be taken for the Project including the following sections:

- Company Introduction and Overview
- Project Approach
- Proposed Solution to meet System Capability Requirements in Appendix A

5.3.3 Resumes
Include individuals your organization will commit to the Project, including any planned sub-contractors. Please note any individuals located in the Columbus, GA area with ability to provide on-site support.

5.3.4 List of Relevant Projects
Provide examples of projects that include the proposed Solution and highlight the results obtained for the customer. Federal- or DoD-specific projects are preferred.

The proposal must also indicate whether the vendor is authorized to conduct business in the State of Georgia.

**5.4 Evaluation Criteria**

Proposals will be reviewed through a formal evaluation process that considers the evaluation criteria shown in Table 3. Should evaluators have questions about particular proposals, US Ignite has discretion to initiate an informational interview with proposing organizations.

US Ignite will evaluate proposal using the following criteria:

**Table 3 - Evaluation Criteria**

| Criteria Description | Weight |
|---|---|
| **Approach** - Proposal clearly communicates how the proposal meets the project requirements and how the solution will be implemented | **20%** |
| **System Capability Requirements** - Quality of remote surveillance data provided by proposed solution | **30%** |
| **Experience** - Company and personnel have demonstrated the ability to complete projects of this scope and technical content | **30%** |
| **On-site Support** - Ability of proposer to provide on-site support at Fort Benning | **10%** |
| **Small Business Concerns** - see below | **10%** |

Per US Ignite Federal Contracts and Grants Management Policies and Procedures, US Ignite will make

efforts to use disadvantaged businesses, including small businesses, minority-owned firms, women's business enterprises, and firms in labor surplus areas, whenever possible and per 2 CFR 200.321. Therefore, 10% of the evaluation criteria will be provided to proposals that involve a prime organization or subcontractor organization that qualifies as a Small Business (SB), Small Disadvantaged Business (SDB), 8(a) Certified SDB, Historically Underutilized Business Zone Small Business (HUBZone SB), Service-Disabled-Veteran-Owned Small Business (SDVOSB), or Woman-Owned Small Business (WOSB)." and keep the table.

**Table 4 - Small Business Concerns**

| Small Business Concerns | Total Contract Percentage/Total Contract Value | Name of Small Businesses/Small Business Concerns Involved in Proposal |
|---|---|---|
| Please provide the percentage % and total contract value that $ will be committed to one or more of the following: Small Business (SB), Small Disadvantaged Business (SDB), 8(a) Certified SDB, Historically Underutilized Business Zone Small Business (HUBZone SB), Survive-Desabled-Veteran-Owned Small Business (SDVOSB), or Woman-Owned Small Business (WOSB) concerns | %<br>$ | |

## 5.5 Other Terms and Conditions

1. Authority to Transact Business in Georgia: Each Proposer shall be able to provide documentation that confirms that the Proposer is authorized to conduct business in the State of Georgia.

2. Master Services Agreement and Task Order: If US Ignite elects to make an award(s) to a Proposer(s), then US Ignite will prepare and send a Master Services Agreement (MSA) and Task Order(s) to the successful Proposer(s). No award will be finalized without a fully executed MSA.

3. No Offer by US Ignite: This RFP does not constitute an offer by US Ignite to enter into an agreement. This RFP is simply an invitation for offers from interested Proposers. No offer shall bind US Ignite.

4. Accept and Rejection of Proposals: US Ignite may reject any or all proposals in whole or in part, waive a technicality, make awards in a manner deemed in the best interest of US Ignite and unless otherwise specified by the organization, accept any item in the proposal.

5. Multiple Awards: US Ignite reserves, at its sole discretion, the option to make awards to multiple Proposers. Multiple awards may be made on the total Scope of Services or components of the Scope of

Services.

6. Ownership of Proposals: Each Proposal submitted to US Ignite will become the property of US Ignite, without compensation to a Proposer, for US Ignite use. US Ignite will not share proposals with any individuals or entities outside of the US Ignite review team and its key project stakeholders - ERDC and Fort Benning. Proposers should mark any proprietary information within the proposal.

7. Limit of Insurance Coverage shall be at least:

Commercial General Liability (CGL) - Products and completed operations, property damage, bodily injury, and personal & advertising injury with limits no less than $1,000,000 per occurrence, and a general aggregate with limit no less than $2,000,000.

Automobile Liability - Insurance Services with a limit no less than $1,000,000 per accident for bodily injury and property damage.

Workers' Compensation insurance - Employer's Liability Insurance with a limit of no less than $1,000,000 per accident for bodily injury or disease.

Cyber Liability Insurance - Limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in the agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

8. Additional Policies: Please note that the Proposer may need to access Fort Benning and would need to follow Fort Benning's Access Control Policies. Individuals that do not have a Department of Defense (DoD) Identification (ID) Card and require entry onto Fort Benning Installation will be subjected to a National Crime Information Center Check (NCIC Check). The individual must have a valid U.S. or State issued photo ID, or U.S. Passport to show for proof of identity. If the individual is driving a vehicle, he/she must have a valid driver's license with current registration and insurance for the vehicle being driven on the installation. All identification presented must meet the requirements of the Real ID Act. All persons requesting unescorted access will continue to be vetted through the NCIC prior to being issued a locally produced ID or pass. If a visitor requesting access does not have a REAL ID Act compliant form of identification and cannot provide supplemental identity proofing documents, they must be escorted at all times while on the installation. Vendors will only be granted access onto Fort Benning Installation if the NCIC III check on the individual shows no disqualifying issues in the check.

# Appendix A - System Capability Requirements

The following system capabilities listed as “must-have” define the minimum functional requirements of the Final Design solution. Additional “may-have” capabilities describe desired functionality that may be included to enhance the proposal over the minimum requirements. Proposers are encouraged to elaborate on capabilities that may not explicitly be listed or note requirements that are not applicable to their solution.

## A.1 System Architecture

The system must be integrated to at least some extent with the SICD, which will be hosted within the underlying Garrison COP platform tenant within a Microsoft Azure Government cloud. This is necessary so that if the pilot project is successful, the vendor solution may be scaled across other installations in the Army Enterprise that leverage this Garrison COP. Please include a brief description and architecture diagram outlining how the proposer’s solution is expected to integrate with the SICD. (i.e. “all of the required subsystems of the proposed solution will be contained within the vendor private cloud, and will integrate just the IAM service with the SICD” if that is the proposed architecture.)

*Must-Have*

- At a minimum, the vendor solution must leverage the identity/access management service provided by the Garrison COP. More details on this requirement may be found in section 4.1.10.
- If a vendor private cloud is proposed, it must be fully or provisionally FedRAMP approved or have gone through the DoD Cloud Authorization Process, or be capable of obtaining approval during the project. This is so that a connection between the vendor private cloud and the Microsoft Azure Government Cloud may be established, and so that government data may be stored on the private cloud if that is part of the proposed solution.

*May-Have*

- The vendor may propose how much of the overall system architecture they will develop or have already developed, and how much would need to be developed by US Ignite.
- The vendor may propose how much of the overall system architecture they anticipate being hosted within their managed environment (whether at the edge or in their data centers or virtual private cloud), and how much of the overall system architecture they anticipate being hosted within the Azure Government Cloud. This is conditional on the vendor’s solution minimally meeting the ‘must-have’ requirements described throughout section 4.1.
    - As an example, two potential architectures are provided below articulating opposite ends of the spectrum of shared development/hosting responsibility between the vendor and US Ignite/ERDC.
    - Shown in Figure 1, the vendor solution may provide the edge sensing, computer vision and backhaul capabilities, and US Ignite may be responsible for developing and hosting the back-end application, front-end application, messaging services, and other subsystems.
    - Shown in Figure 2, the vendor solution may include provision and hosting of all the necessary subsystems, and minimally leverage the Identity/Access Management service provided within the Azure Government Cloud.
- The vendor may propose a preliminary architecture in their proposal, and they may indicate that the final architecture will be decided subject to discussion during the design phase.

**Figure 1 - Remote Surveillance Architecture Example 1 - US Ignite hosted/developed**

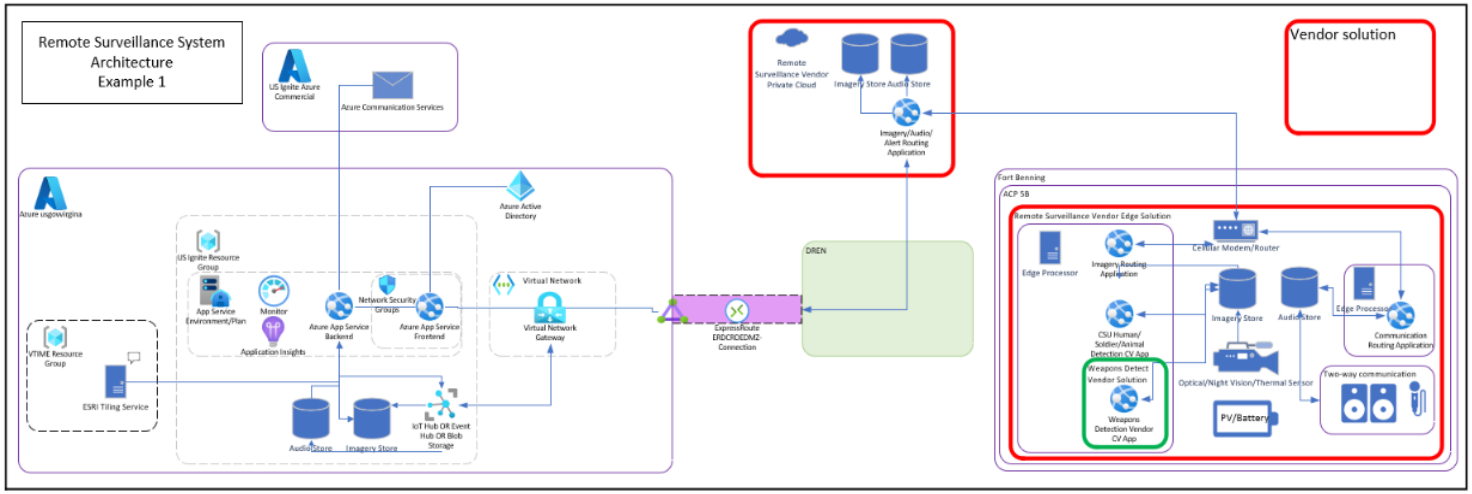
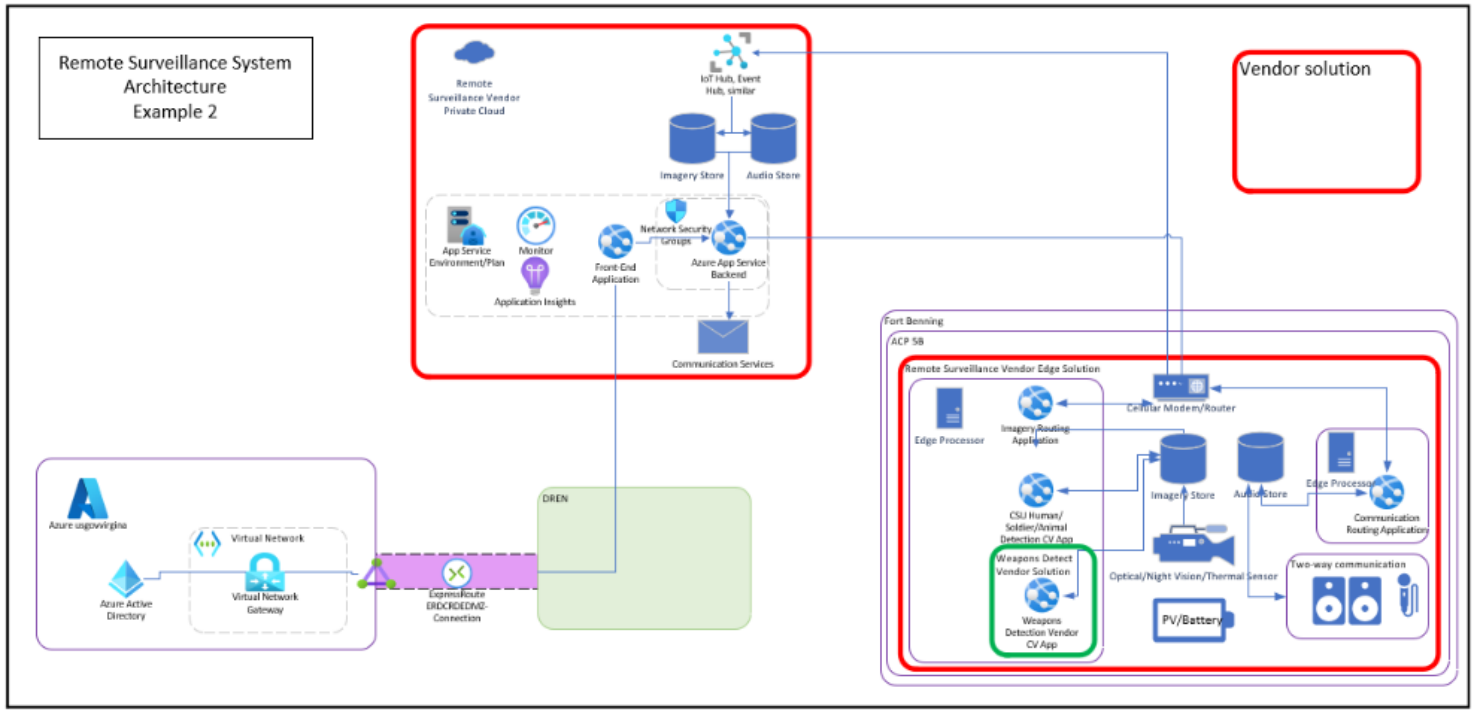



**Figure 2 - Remote Surveillance Architecture Example 2**


Remote Surveillance System Architecture Example 2
Remote Surveillance Vendor Private Cloud
IoT Hub, Event Hub, similar
Imagery Store
Audio Store
App Service Environment/Plan
Monitor
Application Insights
Front-End Application
Network Security Groups
Azure App Service Backend
Communication Services
Vendor solution
Fort Benning
ACP 5B
Remote Surveillance Vendor Edge Solution
Edge Processor
Imagery Routing Application
Cellular Modem/Router
Imagery Store
Audio Store
Edge Processor
Communication Routing Application
CSU Human/ Soldier/Animal Detection CV App
Weapons Detect Vendor Solution
Weapons Detection Vendor CV App
Optical/Night Vision/Thermal Sensor
PV/Battery
Two-way communication
Azure usgovvirginia
Virtual Network
Azure Active Directory
Virtual Network Gateway
ExpressRoute ERDCRDEDMZ-Connection
DREN

## A.2 Sensing Capabilities

The pilot location where the remote surveillance system will be deployed includes paved roads, low buildings, open lots, chain link fencing and heavily wooded parcels. The area is bordered by public facilities and private land. Surveillance into these adjacent areas is not permitted. In general, the areas identified for remote surveillance by FBGA have limited activity during operational hours and little-to-no activity after hours.

*Must-Have*

1. Optical/daytime camera
2. Night-vision camera
3. Thermal camera
4. The ability to detect human size targets at 300 meters using one or more cameras
5. A means of restricting surveillance to a certain field of view

*May-Have*

Columbus State University is training offline soldier and animal detection computer vision algorithms using cameras with the specifications below. These exact cameras are not required to be proposed, but sensors with comparable specifications would be ideal so that their algorithm may be deployed using imagery from the proposed cameras.

6. Optical and night-vision camera
    - 1920 x 1080 (2-Megapixel)
    - Recognition Day: 3 Km (9800 ft. 1.8 miles)
    - Recognition at night using IR: 500m (1600 ft.)
    - Color : 0.02 lux (1/30 sec, F1.6), B/W : 0.002 lux (1/30 sec, F1.6), 0 Lux (IR LED On and in range)
7. Thermal camera
    - 320 x 240 thermal resolution, 9Hz
    - Field of view: 24°x 18°
    - Operating temperature range: -13°F to +131°F (-25°C to +55°C)
    - Pan, tilt and electronic zoom
    - Detects human size target at 559 meters

Additional sensing capabilities may be proposed, including the following:

8. White phosphor sensing technologies
9. LiDar/Radar
10. The ability to operate in all-weather conditions including high winds, heavy snow, rain, and fog
11. Sensors deployed at multiple locations to increase the overall range, or provide coverage in uniquely shaped areas
12. Advanced sensing technologies that include vibration, electromagnetic, wireless device detection, signal scanning, etc.

## A.3 Edge Processing/Computer Vision/Intelligent Video Analytics

Columbus State University will be developing a computer vision (CV) algorithm to detect humans, soldiers, and animals that will utilize imagery data from the cameras and is expected to be hosted on the edge processing devices of the proposed solution. The selected Proposer is expected to support the deployment of CSU's algorithm onboard its edge processors and support its integration with the associated imagery feeds.

If proposers are able to source a comparable algorithm that has already been developed, that may be proposed. Additionally, vendors may propose computer vision algorithms for detecting weapons on individuals, including firearms, bladed weapons, and more to be proposed by the vendor.

*Must-Have*

- The proposed solution must include edge processing, either on the device or within the same local network, sufficient to support two parallel computer vision algorithms being deployed using input imagery data.

*May-Have*

CSU is currently training soldier and animal detection computer vision algorithms using edge processing devices with the specifications below. These exact devices are not required to be proposed, but edge processors with comparable specifications would be ideal so the algorithm may be deployed with comparable performance to the test environment.

- Jetson Xavier NX Developer Kit
    - GPU: NVIDIA Volta architecture with 384 NVIDIA CUDA® cores and 48 Tensor cores
    - CPU: 6-core NVIDIA Carmel ARM®v8.2 64-bit CPU 6 MB L2 + 4 MB L3
    - Memory: 8 GB 128-bit LPDDR4x @ 51.2GB/s
    - Storage: microSD
- Jetson AGX Xavier Developer Kit
    - GPU: 512-core Volta GPU with Tensor Cores
    - CPU: 8-core ARM v8.2 64-bit CPU, 8MB L2 + 4MB L3
    - Memory: 32GB 256-Bit LPDDR4x | 137GB/s
    - Storage: 32GB eMMC 5.1

Additional edge processing/intelligent video analytics capabilities may be proposed, including the following:

- Computer vision algorithms for detecting individuals, soldiers, vehicles, animals, and other objects
- Computer vision algorithms for detecting weapons on individuals, including firearms, bladed weapons, and more to be proposed by the vendor

## A.4 Additional Peripherals and Features

Proposers are encouraged to include additional peripherals and features in the proposals based on industry best practices, unique or advanced functionality available, or novel approaches that meet the objectives of the project. Some examples of these include, but are not limited to:

1. Talk-down or two-way speakers with recording capabilities
2. Motion-activated lights or other local alarms
3. Shot spotting or active shooter technology
4. Counter-UAS detection and deterrence capabilities, whether through computer vision or other sensing capabilities
5. Vehicle fleet tracking capabilities for public safety vehicles to be integrated into the Garrison COP
6. Cellular or wifi wireless device detection
7. Theft prevention
8. Facial recognition, gait analysis, travel trajectory prediction
9. License plate recognition
10. Additional peripherals may be proposed by the vendor

## A.5 Network/Backhaul

*Must-Have*

- The proposed solution must provide backhaul to either the proposer's private cloud or to the Azure Government cloud depending on where the application will be hosted.
- If the application is hosted within the proposer's private cloud, the proposer must establish a connection with the Azure Government cloud during the project in order to leverage the Identity/Access Management service that will be hosted there.
- If the application is proposed to be hosted within a vendor private cloud, that cloud must be fully or provisionally FedRAMP approved or have undergone the DoD Cloud Authorization process so that a connection can be established with the Microsoft Azure Government cloud.

## A.6 Front-End Application

The front-end application presented to FBGA and community law enforcement officials may be adopted as-is from the proposer if it meets the requirements below. Alternatively, it may be developed entirely by US Ignite, or the proposer's off-the-shelf application may be customized to meet these requirements. Proposers must provide an example of their off-the shelf user interface/front-end application if available, and an assessment of the customization/integration work necessary by US Ignite to meet these requirements.

*Must-have US Ignite or vendor-developed front-end application requirements:*

1. The front-end application must be web accessible by desktop, mobile, and tablet devices.
2. The front-end application must include a banner of active alerts of possible intruders detected, including the following features
    a. date/time of detection
    b. warning level (alert if intruder detected, warning if group, weapon or UAS detected)
    c. Intervention recommended (this is static)
    d. Current reviewer (dynamically changes as reviews/actions are taken by stakeholders in

the intruder identification/deterrence process)
   e. Location of detection
3. The front-end application must include a panel with tabs for each of the monitored locations, which may be expanded to include detection details (if available)
4. The front-end application must include play, pause, and playback capabilities for all imagery in which potential intruders were detected.
5. The front-end application must support switching between proposed sensing capabilities (optical/night vision/thermal, etc.)
6. The front-end application must include a map providing the location of the monitored region and the position of the potential intruder at the time each image was taken.
7. The imagery shown in the front-end application must include the bounding box of the object identified as a potential intruder.
8. The front-end application must support the sharing of intruder detection details between stakeholders involved in the intruder identification/deterrence process through SMS and email.
9. The front-end application must include a historic log of intruder detection incidents, including video/audio playback, associated parties, date/time, location, and more to be proposed.
10. The front-end application must be consistent with the US Army visual styling standards applied across SICD and Garrison COP use cases.

## A.7 Back-End Application

The back-end application managing the business logic of the capability may be adopted as-is from the proposer if it meets the requirements below. Alternatively, it may be developed entirely by US Ignite, or the proposer's off-the-shelf application may be customized to meet these requirements. Proposers must provide a description of their back-end application, the languages it was written in and any dependencies (if available), and an assessment of the customization/integration work necessary by US Ignite to meet these requirements.

*Must-have US Ignite or vendor-developed back-end application requirements:*

1. The back-end application must include system monitoring, health, and fault alerting services for all applicable subsystems
2. The back-end application must manage the business logic of routing between the front-end application, managing the processing of detection alerts, data storage, and sms/email communication services
3. The back-end application must manage the business logic of alerting initial dispatch personnel via sms/email when potential intruders are detected
4. The back-end application must manage the routing of users through the appropriate log-in forms
5. The back-end application must support the approval and customization of dispatch messages being sent to law enforcement personnel, and the customization of intended message recipients.
6. The back-end application must manage the business logic of modifying alert objects when they've been approved for dispatch, including the time dispatched, custom messages, and dispatch recipients.
7. The back-end application must manage the business logic of personnel entering after-action reports associated with particular intrusions.
8. The back-end application must manage the business logic of presenting a log of historic alerts and information associated with them to the front-end application.

9. The back-end application must manage the business logic of user group/role management and administration, including adding, modifying, and deleting users.

## A.8 Data Acquisition and Storage

*Must-Have*

1. At least the most recent 3 days of continuous video data must be cached either on edge device or in private cloud
2. All incidents of objects being detected or two-way audio (if captured) must be stored for perpetuity
3. Data must be retrievable through the front-end application by individuals with appropriate credentials to support deterrence and litigation efforts, whether the application is served within the vendor private cloud or the Azure Government Cloud
4. Data must be made accessible via API to users of the Microsoft Azure Government cloud with appropriate credentials.
5. If data is proposed to be stored in or transmitted through a vendor private cloud, that private cloud must be fully or provisionally FedRAMP approved or have gone through the DoD Cloud Authorization Process, and it must be certified to store data commensurate with the impact level (IL) classification of the imagery and metadata captured.

## A.9 Alerting/User notifications

The application must notify Fort Benning law enforcement personnel by email and text message when a potential intruder has been detected by the system, and it must also support dispatch officers sharing detection details with other law enforcement personnel to aid in their deterrence of detected individuals. This capability may be adopted as-is from the vendor if it meets the requirements below. Alternatively it may be developed entirely by US Ignite, or the vendor's off-the-shelf application may be customized to meet these requirements. Proposers must provide a description of the alert/messaging services supported, the languages or API's they rely on (if available), and an assessment of the customization/integration work necessary by US Ignite to meet these requirements.

*May-Have*

- The vendor solution may include text message/email alerting services for sharing detection details between intruder identification/deterrence stakeholders, or they may be deployed by US Ignite using Azure Communication Services.

## A.10 Identity/Access Management

The users of this system will include both Fort Benning military law enforcement personnel, as well as local non-military law enforcement personnel and impacted civilian stakeholders.

For military personnel, the Identity/Access Management (IAM) service of the vendor's solution must be capable of authenticating access with their credentials within the Azure AD service hosted within the Microsoft Azure Government cloud. This AD service only authenticates military credentials and does not manage user groups, roles or permissions, and so the vendor's IAM service must manage these details of each user within their IAM service. The vendor must propose a preliminary approach to federating their

IAM service with the Azure Government cloud IAM service in order to associate military credentials with their groups/roles, potentially using the B2B Direct Connect or B2B Collaboration Azure services. This preliminary approach may be refined and confirmed following contract execution, prior to critical design review.

For non-military personnel, the vendor's solution must manage the authentication of user's credentials, as well as their groups/roles and permissions.

## A.11 Installation and Functional Specifications

Given the short duration of the pilot, a quickly deployable, temporary or semi-permanent installation is preferred. This also allows for relocation of the system if the orientation or placement of the solution needs to be adjusted during operations. Generally speaking, the system should be self-sustaining and not require site modifications, power or communications to operate.

*Must-Have*

- Mechanical Specs - proposals must include the physical dimensions of the system in its deployed state
- Environmental Specs - the proposed solution will be deployed outdoors and is subject to four seasons of subtropical climate and seasonal rain (45-75 inches), tropical cyclones, and temperatures (60-105 °F) typical of the region
- Power - the proposed solution must be self-sustaining through a combination of battery, solar, or other technologies as power will not be available in the remote locations of FBGA
- Deployment - the proposed solution must be quickly deployable and not require major site modification for installation. A semi-permanent installation utilizing poles is acceptable.

*May-Have*

- Power - basic electrical service may be available in some areas so the proposed solutions may include a direct power option.

## A.13 Cyber Security Requirements

As a research and development project the solutions demonstrated during this pilot will not need to undergo authority to operate (ATO) authorization during the project, but proposed solutions should be capable of undergoing such authorization in order to be scaled in the future. While NDAA compliant equipment is not required for the pilot, proposers should include documentation on the current level of compliance and what would be required to be fully compliant for scaling future permanent solutions.

*Must-Have*

- Proposers must support the determination of the DoD Impact Level classification of the collected data to determine whether it may be stored and processed in the Azure GovCloud or vendor private cloud (as applicable).
- Edge devices must include physical security such that critical data storage, processing, and power systems may not be accessed, tampered with or otherwise compromised.
- All data must be minimally 256-bit encrypted in edge storage and transport.
- Access to edge devices must be restricted to authorized users.

*May-Have*

- Proposed solutions may include AI-driven cyber anomaly detection services for monitoring for malicious system traffic.

# Appendix B - Scope of Services During Project Phases 2-4

## B.1 Project Schedule

| Deliverable | Project Phase | Target Suspense | Content |
|---|---|---|---|
| Remote Surveillance System Deployed | Phase 2: System Installation | 2/10/2023 | Deliver, install and operationalize the surveillance system Installation After-action report |
| Operations | Phase 3: Operations | 2/24/2023 | Achieve steady-state operations, Complete operational test plan |
| Week/Bi-weekly Meetings | Phase 1-3: System Integration Support | 11/1/2023 - End of PoP | Participate in weekly or bi-weekly program meetings with stakeholders remotely or in-person as needed. |
| The solution's O&M costs OR the decommissioning plan and cost | Phase 4: Decommissioning and/or Annual O&M Support | 11/1/2023 | |
| The final project report | Phase 4: Decommissioning and/or Annual O&M Support | 11/30/2023 | The overall work completed, comparison to the SoW, findings, recommendations, and an executive summary |

## B.2 System Installation: Phase 2

- The selected Proposer will install, connect and operationalize the proposed remote surveillance system at FBGA in the pilot location.
- After the installation is complete, an after-action report must be submitted detailing any divergences and key findings from the installation.

## B.3 Operation: Phase 3

- The selected Proposer must develop an operational test plan with agreed upon key performance indicators once all computer vision and other subsystems are developed, tested and integrated. They must complete the operational testing period and successfully deliver the performance requirements. This operational test plan must include:
    - confirmation that CSU's computer vision algorithm has been successfully deployed onboard edge processing devices
    - confirmation that objects detected by CSU's computer vision algorithm trigger an sms/email alert to dispatch personnel

  - confirmation that validation of intruders detected and approvals of dispatch get sent by SMS/email to law enforcement personnel, and that the associated alert object is updated accordingly by the back-end application
  - confirmation that the front-end application meets the requirements specified in section A6.
  - confirmation that after action reports submitted through the front-end application are managed appropriately by the back-end application and persist for future recall
  - confirmation that all video imagery associated with intrusions may be accessed at a later date, and that all imagery in the last three days may be accessed.
  - Other unit and system readiness tests to be proposed by the vendor
- Provide a monthly brief to US Ignite capturing the work completed, risks and mitigation strategies, issues encountered and planned activities.

## B.4 System Integration Support: Phases 2-3

The selected Proposer must support the deployment of partner subsystems that interface with the proposer's system. This includes providing documentation on the OS, available libraries, and other resources necessary for computer vision applications developed by US Ignite and their partners to be deployed on the edge devices. This also includes provision of proper API documentation for all subsystems developed by the proposer.

The selected Proposer is expected to support this activity by:

- Participate in weekly or bi-weekly program meetings with stakeholders remotely or in-person as needed.

## B.5 Decommissioning and/or Annual Operations and Maintenance Support: Phase 4

The desired outcome for the project is to leave the proposed solution in place to operate beyond the end of the contracted period of performance. Therefore, ongoing operation and maintenance (O&M) will be considered when evaluating the long- term viability of the proposal.

If FBGA does not want to assume control, or continue to lease the Proposer's installed equipment at the end of the project, the Proposer may be required to decommission the system and return the site to its original condition. This decommissioning plan and cost must be included in the proposal description.

Deliver a final project report describing the overall work completed as compared to the agreed upon scope of work. The report should include findings, recommendations, and an executive summary.