

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

I. Background and Purpose

The U.S. Army is seeking innovative electromagnetic spectrum operations solutions from eligible small and large businesses across the globe through the Global Tactical Edge Acquisition Directorate (G-TEAD) U.S. Army Europe and Africa (USAREUR-AF) Accelerated Capability Event (ACE) 27-02 Spectrum Enabled Warfare Powered by xTech competition. This platform offers participants the opportunity to engage with the U.S. Department of War (DoW), earn prize money and submit a proposal for follow on contract opportunities.

The U.S. Army FUZE xTech Program, managed under the Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)), in partnership with USAREUR-AF and G-TEAD, is executing the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition as part of the G-TEAD ACE series.

This initiative supports the U.S. Army's broader effort to (1) identify and understand the spectrum of 'world-class' technologies being developed commercially that benefit the U.S. military; (2) integrate non-traditional innovators into the U.S. DoW Science and Technology (S&T) ecosystem; (3) provide expertise and feedback to accelerate, mature, and transition technologies to support operational forces; and (4) deliver attritable, scalable capabilities.

The G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition will consist of three (3) phases:

- (1) Application, including the following:
 - a. Four (4)-page white paper;
 - b. Required five (5)-minute video;
 - c. Self-certification of minimum requirements; and
 - d. Information on prior demonstrations with DoW or allied/partner nations
- (2) Soldier exercise; and
- (3) Opportunity to submit follow-on contract proposal.

The U.S. Army intends to **award up to \$1,500,000 in cash prizes** throughout the competition. **Up to 15 finalists will be selected at the conclusion of the Part 1 evaluation period** for an opportunity to participate in the Part 2 live Soldier exercise, anticipated to occur in February or March 2027. **Finalists who attend the Soldier exercise will receive a cash prize of \$25,000 each, following the event. Finalists who also participate and have their technology integrated in the exercise will receive an additional \$25,000 each, following the event.** Following completion of the exercise, up to five (5) final winners will be selected to receive an additional cash prize of \$150,000 each and may be considered for potential follow-on agreements and contracting opportunities. Additional details on prize structure can be found in Section VII.

At the Government's discretion, participants that do not win a prize may also be considered for opportunities to demonstrate their capability.

Finalists and final winners addressing capability areas 1-3 that qualify as a U.S. Small Business will have the opportunity to submit a Direct to Phase II (DP2) Army Small Business Innovation Research (SBIR) proposal worth up to \$2,000,000, not to exceed 18 months in duration. Finalists and final winners that do not meet the U.S. Small Business eligibility requirements, or those entities (small or large businesses) that address capability area 4 will not be eligible for the SBIR opportunity but will be eligible to submit proposals for other follow-on opportunities.

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

Eligibility to submit does not guarantee award.

Any follow-on agreements are at the Government's sole discretion and are subject to availability of funds and applicable laws and regulations. Nothing in this solicitation shall be construed as a commitment to issue a request for proposal (RFP) or award any contract or agreement.

Finalists and final winners must have a CAGE/NCAGE code to receive a cash prize and contract award. A CAGE/NCAGE code is not required at the time of application; however, applicants that do not possess one (1) are strongly encouraged to initiate the registration process in advance if they intend to participate.

The G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition is conducted in accordance with 10 U.S.C. § 4025, which authorizes the use of prize competitions to stimulate innovation and identify promising technologies for national security applications. Requirements for competition under 10 U.S.C. § 3201 are satisfied upon completion of the challenge and use of prize authority. As such, this competition serves as a competitive down select mechanism that enables government organizations to engage with finalists and winners through a variety of follow-on acquisition pathways, including but not limited to:

- 10 U.S.C. § 4114 – Selection of contractors for prototype projects
- 10 U.S.C. § 4022 – Prototype projects
- 10 U.S.C. § 4023 – Procurement for experimental purposes
- 10 U.S.C. § 4001 – Research and development
- 10 U.S.C. § 4021 – Other Transaction Authority (OTA)
- 10 U.S.C. § 3458 – Authority to acquire innovative commercial products and commercial services using general solicitation competitive procedures
- 15 U.S.C. § 3703 – Technology innovation partnerships
- 15 U.S.C. § 638 – SBIR and Small Business Technology Transfer (STTR) Programs

Government organizations may consider leveraging these statutory authorities to pursue follow-on awards with companies identified through the xTech competition process. This approach supports rapid technology maturation, accelerates the transition of innovative capabilities to the field, and promotes collaboration with non-traditional and small business performers.

While the authority of this program is 10 U.S.C. § 4025, the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition may generate interest by other U.S. Army, DoW or U.S. Government (USG) organizations for a funding opportunity outside of this event. The interested organization may contact the participant to provide additional information or ask for a request for proposal in a separate solicitation. Finalists of the prize competition may have opportunities to submit a separate proposal for further development of their proposed technology solution based on the needs of the Army. The Army may use a contract mechanism of their choice and will notify the participants accordingly.

All G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition submissions are treated as privileged information and contents may be disclosed to employees of the USG, allied nations, designated support contractors at the USG's discretion for the purposes including, but not limited to, evaluation, program administration and support, potential inclusion in Army or DoW marketplaces, and consideration for potential follow-on opportunities. The Government will use reasonable efforts to protect proprietary information; however, participants are responsible for

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

clearly identifying any proprietary or restricted information within their submissions.

The Army FUZE xTech Program intends to provide feedback from evaluators to participants during each part of the competition. The purpose of providing this feedback is to help accelerate the transition of the technology to a U.S. Army end-user by providing insight into the best applications for the technology, suggestions for product improvement for U.S. Army use and recommended next steps for development. However, the Government will not respond to inquiries regarding this feedback.

II. Eligibility Requirements

General Eligibility (All Applicants)

Eligible entities include nonprofit organizations, for-profit organizations (i.e., large and small businesses) both domestic and foreign.

Each eligible entity:

- Must be able to obtain a CAGE code (U.S. businesses) or NCAGE code (international businesses) to process payments and receive follow-on awards;
- Shall be incorporated in, and maintain, a primary place of business in the U.S. or an allied foreign country;
- Shall not be a U.S. Federal Government entity, foreign government entity or employ a U.S. Federal Employee acting within the scope of their employment;
- Shall not be currently under contract, agreement or other providing similar capabilities in the region under the same use case to the Government for work described in the problem statement; and
- Must not be based in a Foreign Country of Concern (FCOC), directly funded by an FCOC government or government-subsidized guidance fund, or under the influence of an FCOC government in any form.

U.S. Small Business Eligibility (for potential Army SBIR opportunity)

Small, for-profit, independent U.S. businesses. Restrictions exist about (1) the type of firm; (2) its ownership structure; (3) the firm's size in terms of the number of employees; and (4) prior, current, or pending support of similar proposals or awards, as follows:

- (1) Type of Firm: An eligible firm must be organized as a for-profit concern and meet all the other small business requirements in 13 C.F.R. § 121.702. Non-profit entities are not eligible.
- (2) Ownership and Control: A majority (more than 50%) of an eligible firm's equity (e.g., stock) must be directly owned and controlled by one (1) of the following:
 - a. One (1) or more individuals who are citizens or permanent resident aliens of the U.S;
 - b. Other for-profit small business concerns (SBCs) (each of which is directly owned and controlled by individuals who are citizens or permanent resident aliens of the U.S.);
or
 - c. A combination of (a) and (b) above.

Note: If an employee stock ownership plan owns all or part of the concern, each stock trustee and plan member is considered an owner. If a trust owns all or part of the concern, each trustee and trust beneficiary is considered an owner.

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

- (3) Size: An eligible firm, together with the affiliates, must not have more than 500 employees.
- (4) Prior, Current, or Pending Support with Similar Technology: Proposals submitted in response to this prize competition must not be substantially the same as another proposal that was funded, is now being funded, or is pending contract award with another federal agency. **Small businesses with any questions concerning prior, current, or pending support for similar proposals or awards must disclose those as early as possible to the Army FUZE xTech Program Office.**

Other Eligible Entities

Eligible entities not qualifying as a U.S. Small Business may include domestic and foreign for-profit organizations, non-profit organizations, and large businesses, provided they meet all general eligibility requirements listed above.

Failure to meet any of the above requirements will result in ineligibility for award. The USG reserves the right to verify eligibility and make all final determinations at its sole discretion.

III. Topics and Problem Statement

The operational challenge on the Eastern Flank is the enablement of U.S. Army forces, operating within a North Atlantic Treaty Organization (NATO) and joint coalition framework, to sense, understand, exploit, attack, and protect across a contested electromagnetic environment and connected cyberspace. To deter peer aggression and preserve freedom of maneuver, V Corps must protect tactical command and control networks while delivering synchronized, non-lethal and lethal effects at depth against adversary command, control, communications, and targeting architectures.

Gaining and maintaining spectrum superiority against dense anti-access / area denial systems requires a modular, coalition-interoperable architecture that operates in congested radio frequency (RF) environments, executes multi-echelon precision effects, and hardens friendly formations against persistent electromagnetic and cyber disruption during competition, crisis, and conflict. The Army requires capabilities that are scalable, upgradeable, intuitive for Soldiers across military occupational specialties, and maintainable at the tactical edge without routine reliance on field service representatives for minor repairs or adjustments.

The Army is seeking to evaluate capabilities that demonstrate performance in one (1) of four (4) capability areas, and meet the following criteria for its capability area:

- **Capability 1:** [Electromagnetic Support / Tactical Surveillance](#)*
- **Capability 2:** [Autonomous Network Management](#)*
- **Capability 3:** [Electromagnetic Environment Visualization and Battle Damage Assessment Tools](#)*
- **Capability 4:** [Electromagnetic Attack & Active Countermeasures](#)

*Note: SBIR|STTR funding opportunities will be limited to finalists and final winners addressing capability areas 1-3.

For details on the full capability areas, see [Appendix A](#).

Capabilities submitted for evaluation **shall meet** the following criteria, as applicable:

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

- TRL 6 or higher;
- Clear linkages to resolving the problem statement and meeting the desired characteristics for the capability gap in which technology will compete;
- Demonstrate viability to field solutions within 180 days of contract award.
- The overall system architecture shall minimize proprietary dependencies and enable rapid integration with successor systems without significant redesign or vendor-unique middleware.
- Systems shall utilize non-proprietary, commercially driven, widely accepted, consensus-based open standards where all software-reliant interfaces are exposed as application programming interfaces (APIs), or similar commercial standards applicable to the technology such as remote procedural calls, message queues, or web sockets.
- The capability shall demonstrate the ability to securely ingest, publish, and exchange operational data—including, but not limited to: situational awareness, system status, mission tasking, system telemetry, operational data streams, and control functions.
- Systems shall demonstrate compatibility with the EFDI Data Backbone, as detailed in Appendix B, by:
 - (a) enrolling the system as an authorized peer in the Backbone's WireGuard mesh overlay via the Government-designated mesh control service (NetBird), and
 - (b) as applicable to the system, publishing and/or subscribing to event-driven data over the Government-designated publish/subscribe protocol (Zenoh), and exchanging control commands as request/response with an explicit reply.
- Capable of operating in a denied, degraded, intermittent and limited GPS and communications environment;
- Demonstrate cyber resilience and compliance;
- Demonstrate assured control in contested environments;
- Provide safe, predictable behavior around personnel and other unmanned systems, including failsafe mechanisms, obstacle detection / avoidance, and emergency stop behaviors in all modes of operation (remote, tele-operated, autonomous, etc.); and
- Provide on-board diagnostics with operator notification of degraded state (software or sensor failure).

IV. Program Submission

The G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition is voluntary and open to all entities that meet the eligibility requirements listed in Section II (Eligibility Requirements). Entities are encouraged to submit integrated solutions.

Only one (1) submission per eligible company, per capability area is permitted. If submitting to one (1) or more capability areas, the technology solutions must be different, unless submitting an integrated solution.

If submitting an integrated solution, companies must indicate that their solution is integrated when they submit their white paper on the Valid Eval registration page. All submissions must be in English.

NOTE: U.S. Small Business's eligible for potential Army SBIR opportunities will only be permitted one (1) DP2 Army SBIR proposal if selected as a finalist or final winner of this competition. If selected as a finalist or final winner in more than one (1) capability area, the company may choose one (1) proposal to be considered for a DP2 Army SBIR award, and the other winning submission may be considered for other follow-on funding opportunities.

**The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled
Warfare Powered by xTech Competition Announcement**

The registration information and submission upload must be received by **5:00 PM ET on Friday, October 30, 2026**. Submissions received after the deadline will not be considered.

**Register now by selecting the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled
Warfare Powered by xTech competition image at:**

<https://www.xtech.army.mil/>

**V. G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech
Competition Structure**

Part 1: Concept White Paper

All eligible entities shall submit a **four (4)-page concept white paper and pre-recorded video of up to five (5) minutes** that demonstrates the technology and its suitability for participation in a live exercise. The white paper should outline the solution's capability alignment, capability value, system integration, contested readiness, system deployability, ability to field product, and company viability. Submissions will be evaluated by subject matter experts (SMEs) across the U.S. DoW. Any submissions provided above the four (4)-page limit and the five (5)-minute video will not be evaluated.

All concept white papers and videos must adhere to the following requirements:

- Concept white papers **must be submitted using the template found on the [Valid Eval](#) registration page, "Template_ G-TEAD USAREUR-AF ACE 27-02_Spectrum Enabled Warfare Powered by xTech_White_Paper.docx". ***Any proposals submitted in a format other than that provided by the template will not be reviewed.*****
- For the required video, provide a URL on the contest registration linking to the video (preferably hosted on Vimeo). Video production quality will not influence evaluation scores. Videos should serve to clarify or illustrate concepts from the white paper and must not exceed five (5) minutes in length.
- List your company name, country name and proposal title **EXACTLY** how you would like them to appear in any contest marketing materials. Use a clear and concise proposal title to give readers and potential stakeholders an understanding of how your technology would benefit the U.S. Army.
- Proposals by offerors should describe their approach to accomplishment of the expectations using concise narratives.

Evaluators will review and score concept submissions using the following scoring criteria (further details on each scoring dimension can be found on the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition registration page):

Criterion	Weight
Introduction & Capability Alignment	15%
Capability Value	25%
System Integration & Contested Readiness	20%
System Deployability	15%
Ability to Field Product	10%
Company Viability	10%
Submission Quality	5%

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

Upon conclusion of the submission evaluation period, the Army FUZE xTech Program will select **up to 15 finalists who will advance to Part 2: Soldier Exercise.**

Applicants not selected in Part 1 may, at the Government's discretion, be invited to participate in the live exercise event; however, they will not receive a cash prize or be eligible to receive subsequent prize awards under the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition.

Part 2: Soldier Exercise

Selected finalists from Part 1 will participate in a live exercise and pitch event, with a panel of U.S. Army, DoW, and NATO SMEs and end-users. The event is currently expected to be held in February or March 2027, in Germany.

Participation in the Soldier exercise is subject to all applicable safety, security, base access, host-nation, export control, customs, transportation, spectrum, airspace, cybersecurity, and operational requirements. The Government may restrict, modify, suspend, or terminate a participant's exercise activities if necessary to protect personnel, property, networks, mission operations, or compliance with applicable law or policy.

In accordance with the DP2 Army SBIR requirements, each eligible proposing SBC shall provide documentation or demonstrate feasibility of sufficient solution maturity to be eligible for a DP2 Army SBIR award along with the DP2 proposal. Work submitted within the feasibility documentation or demonstration must have been substantially performed by the proposing SBC and/or the principal investigator. If technology in the feasibility documentation is subject to Intellectual Property (IP), the proposing small business concern must either own the IP or must have obtained license rights to such technology prior to proposal submission, to enable it and its subcontractors to legally carry out the proposed work.

Finalists will be required to submit additional documentation prior to the exercise event. These materials are necessary to meet specific safety protocols for Soldiers, export control requirements, network security, and spectrum approval requirements, and to ensure the event is executed successfully. All documentation must be submitted by the stated deadlines. Failure to provide the required materials or meet the deadlines may result in disqualification from G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition.

Participating firms must commit to full participation for the entire duration of the exercise event and must **be on-site** from day one (1) of the exercise event to support Soldier training and meet operational objectives. Non-compliance with event requirements or failure to meet performance standards during the exercise may result in disqualification from the competition.

The Army FUZE xTech Program will provide additional instructions, detailed evaluation criteria, and exact dates and location for the event at a later date.

Prior to the exercise event, finalists will have the opportunity to engage with U.S. Army and DoW personnel to prepare and discuss event expectations.

Dates, times, and location are subject to change.

Upon conclusion of the exercise, the Army FUZE xTech Program will select **up to five (5) final**

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

winners of the competition to receive a cash prize of \$150,000 each, and a potential opportunity to submit for a follow-on contract or agreement. Additionally, finalists may have an opportunity and are encouraged to leave their kits behind to receive additional end-user engagement/feedback with the solutions and enable further opportunities for follow-on contracts or agreements with end-user organizations. Final competition winners may be eligible for an immediate follow-on contract(s) or agreement(s), subject to the availability of funds and technical needs.

Finalists who attend the exercise will receive a cash prize of \$25,000 each and finalists who are able to actively participate and complete all required exercise activities will receive an additional \$25,000 each.

Potential Follow-on Funding Opportunities

Finalists and final winners selected from the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition will be eligible to submit proposals for follow-on opportunities, including but not limited to SBIR, OTA or other procurement or non-procurement instruments, as determined appropriate by the Government.

The Army SBIR|STTR Program will issue eligible U.S. Small Businesses a separate announcement with detailed instructions to submit the DP2 Army SBIR proposal materials. SBIR|STTR funding opportunities will be limited to vendors addressing capability areas 1-3 for the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition.

Finalists and final winners selected from the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition, that meet the U.S. Small Business eligibility requirements, will be the **only firms eligible** to submit a DP2 Army SBIR proposal under this topic. All other submissions will be deemed ineligible. Eligible firms will only be permitted one (1) SBIR DP2 proposal if selected as a finalist or final winner of this competition. If selected as a finalist or final winner in more than one (1) capability area, the company may choose one (1) proposal to be considered for a SBIR DP2 award, and the other winning submission may be considered for other follow-on funding opportunities.

Eligible finalists and final winners will be provided detailed instructions to submit the Army SBIR proposal materials under **Army SBIR Topic “ARM27BX01-DP001”** for a potential follow-on award of up to a maximum of \$2,000,000 and up to an 18-month period-of-performance. This topic can be found on the [Defense SBIR|STTR Innovation Portal \(DSIP\)](#) and will remain in pre-release for the duration of the competition. Upon selecting competition winners, the open submission window for DP2 Army SBIR proposals will be made available.

Other follow-on opportunities, if pursued, may be executed under applicable statutory authorities. Any such opportunities may be subject to separate evaluation criteria, independent selection processes, availability of funds, and all applicable statutory, regulatory, and approval requirements.

Follow-on funding opportunities may require delivery of initial prototypes for evaluation within 45 to 120 days of contract or agreement award that will be used as the initial articles for further experimentation and testing.

VI. Proposed Schedule

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

The proposed schedule is outlined below and subject to change without notice.

Date	Activity
October 14-30, 2026	Part 1: Concept white paper submission period
December 8, 2026	Finalists announced
February/March 2027	Part 2: Soldier exercise event
February/March 2027	Final winners announced
February/March 2027	DP2 Army SBIR proposal submission period

VII. Prizes and Incentives

Prizes will be offered under 10 U.S.C. § 4025 (Prize competitions). The total prize pool is \$1,500,000. **Follow-on contract award/agreements, if issued, will be separate from the prize competition.** Other non-monetary incentives are provided through the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition to help industry engage with the U.S. Army.

Phase	Winners	Prize	Contract Award
Part 1: Concept White Paper	Up to 15	Invitation to Part 2: Soldier exercise event	N/A
Part 2: Soldier Exercise	Up to 5	\$150,000 each Finalists who attend the exercise receive \$25,000 each and finalists who participate in the exercise will receive an additional \$25,000 each	
Opportunity to Submit an Army SBIR Proposal	Up to 5		Total funding pool of up to \$10,000,000
Opportunity to Submit for an OTA	Up to 15		Total funding pool of up to \$6,000,000
	Total	Up to \$1,500,000	Up to \$16,000,000

VIII. Disclaimers

Registered participants shall be required to assume any and all risks and waive claims against the Federal Government and its related entities, except in the case of willful misconduct, for any injury, death, damage, or loss of property, revenue, or profits, whether direct, indirect, or consequential, arising from their participation in this prize competition, whether injury, death, damage, or loss arises through negligence or otherwise.

IX. Intellectual Property

The Army is a strong proponent of deliberate IP rights and management by the private sector and DoW.

For the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

competition:

- The Federal Government may not gain an interest in IP developed by a participant without the written consent of the participant;
- Nothing in this G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech prize competition shall diminish the Government's rights in patents, technical data, technical information, computer software, computer databases, and computer software documentation that the Government had prior to this G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech prize competition, or is entitled to, under any other Government agreement or contract, or is otherwise entitled to under law; and
- The Federal Government may negotiate a license for the use of IP developed by a registered participant in the prize competition.

Register now by selecting the G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech competition tile at:

<https://www.xtech.army.mil/>

X. Point of Contact

The U.S. Army FUZE xTech Program Office
Office of the Deputy Assistant Secretary of the Army, Research and Technology
Email: usarmy.xtech@army.mil
Website: <https://www.xtech.army.mil/>

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

APPENDIX A – G-TEAD USAREUR-AF ACE 27-02 Problem Statements

Capability 1: Electromagnetic Support / Tactical Surveillance

Problem Statement: Modern electromagnetic spectrum operations (EMSO) forces operate in congested and contested electromagnetic environments against sophisticated adversaries employing agile, low-probability-of-intercept/low-probability-of-detection (LPI/LPD) waveforms. This capability area seeks passive sensing solutions that detect, characterize, direction find, and geolocate complex emitters at the tactical edge without producing detectable radio-frequency (RF) signatures or overloading bandwidth-constrained tactical networks.

Solutions shall support the proliferation of low-size, weight, power, and cost sensing assets across maneuver formations, enabling infantry and other non-specialist Soldiers to employ distributed sensors at echelon. The architecture should provide intuitive setup, employment, and status monitoring; minimize dependence on specialized EMSO expertise; and automate sensor configuration, signal processing, correlation, and sensor-tasking functions.

Under disconnected, degraded, intermittent, or limited (DDIL) conditions, solutions shall operate as resilient, edge-capable sensing architectures that process dense signal environments locally and retain essential functionality with limited network connectivity. Desired solutions should support simultaneous detection, location, direction finding, and geolocation of multiple emitters and frequency bands; fuse observations from distributed sensors; and provide low-latency, target-quality data to the common operating picture and multi-echelon targeting workflows.

Desired Characteristics:

- Offerors have wide latitude to propose modular hardware, novel algorithms, hybrid processing architectures, or innovative capabilities across the following operational focus areas:
 - High-Fidelity Passive Sensing & Geolocation: Proposed solutions should maximize Instantaneous Bandwidth (IBW) and dynamic range to detect frequency-agile and LPI/LPD signals, utilizing multi-node, phase-coherent hybrid passive techniques to deliver precision targeting coordinates without active emissions.
 - Autonomous Edge Processing & DDIL Data Resilience: Proposed solutions should execute automated signal characterization, modulation recognition, and antenna polarization identification directly at the edge. Solutions should automate multi-sensor tasking and handoffs while maintaining tracking integrity over severely degraded or low-bandwidth tactical backhaul networks.
 - Maximizing Functionality: Proposed solutions should maximize functionality for sensing across c-UAS, counter-improvised explosive devices (CIED), electromagnetic support (ES) and electromagnetic attack (EA) missions. Systems should include adaptable software and reprogrammable algorithms to characterize evolving target sets.
 - Ease of Use: Proposed solutions shall be operable by Soldiers across military occupational specialties, including infantry Soldiers and other personnel without specialized electronic warfare (EW) training. Systems should use intuitive, standardized user interfaces; minimize required inputs and setup steps; provide

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

clear status indicators and alerts; and enable basic operational training, task-focused training.

- Platform-Tailored SWaP-C Scalability: Proposed solutions shall provide scalable, modular sensing and networking capabilities optimized and scalable across multiple modalities. Solutions must support employment of complementary sensor layers throughout the battlespace, allowing commanders to combine platform-specific capabilities to improve coverage, survivability, persistence, and resiliency.
- Mounted: Provide survivable, on-the-move sensing and networking integrated with tactical ground vehicles. Systems should maintain performance under various vehicle chassis, mobility, and field conditions while supporting persistent coverage along maneuver routes and operational areas.
 - Dismounted/Static: Provide ultra-low visual and radio-frequency (RF) signature, rapidly emplaced, battery-optimized expeditionary sensor nodes suitable for employment by dismounted Soldiers. Nodes should support persistent, unattended sensing where vehicle-based systems cannot operate.
- Ground Robotics: Provide lightweight, low-power payloads for unmanned ground systems that extend sensing into high-risk, restricted, or otherwise inaccessible terrain. Payloads should enable mobile and/or stationary sensing while preserving platform endurance and mobility.
- Group 1–3 UAS: Provide lightweight, low-draw payloads for Group 1–3 UAS that enable elevated or airborne sensing, extend detection range and line of sight, and support rapid repositioning of sensing assets.
- Solutions should enable these modalities to operate independently or as an integrated, distributed sensor network, supporting cross-cueing, data fusion, and graceful degradation when individual sensors, platforms, or communications links are unavailable.

Capability 2: Autonomous Network Management

Problem Statement: Tactical Electromagnetic Spectrum Operations (EMSO) formations operate in congested, contested RF environments where static network planning fails and manual network management overwhelms operators. Operating in Disconnected, Degraded, Intermittent, or Limited (DDIL) environments, the Army requires open, self-healing, and automated network infrastructures capable of autonomously orchestrating distributed EMSO assets, managing spectrum resources, and routing critical sensor-to-shooter targeting feeds without continuous operator intervention. Field training has reinforced that these shortfalls directly affect operational effectiveness when units attempt to integrate systems, move data across formations, and sustain functionality under bandwidth and power constraints.

Desired Capabilities & Innovation Areas:

- Offerors have wide latitude to propose open-architecture software frameworks, distributed orchestration algorithms, or decentralized routing protocols across the following focus areas:
 - Open Systems Architecture (MOSA / SOSA / CMOSS / CMFF): Proposed hardware and software frameworks should adhere to open standards (MOSA,

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

SOSA, CMOSS / CMFF) that reduce-costs, eliminate vendor lock, enable rapid module insertion, and provide seamless, bidirectional data synchronization between enterprise reprogramming pipelines and tactical edge nodes. Solutions should support rapid onboarding of new capabilities, third-party software integration, and intuitive user interaction

- Autonomous Spectrum Management & Dynamic PACE: Algorithmic automation for dynamic spectrum allocation (DSA), automated execution of Primary, Alternate, Contingency, and Emergency (PACE) plans, and self-healing mesh networking to maintain high-availability data routing across contested channels. Proposed solutions should maximize integration with existing tactical and coalition radio networks.
- Distributed Sensor-to-Shooter Orchestration: Edge-native services enabling automated multi-node health monitoring, remote sensor tasking, dynamic sensor-to-sensor handoffs, and low-latency target data delivery directly integrated with next-generation mission command software

Capability 3: Electromagnetic Environment Visualization and Battle Damage Assessment Tools

Problem Statement: Modern electromagnetic spectrum operations (EMSO) forces need real-time understanding of the electromagnetic spectrum (EMS) environment to support decision-making, targeting, and assessment of non-lethal and lethal effects. Commanders and operators need to quickly and simply understand what is happening in the EMS environment, what changed, and whether an effect was achieved without end-user analysis of raw-technical data. Field experience has shown that capabilities that require extensive interpretation or specialized technical expertise create additional burden at the tactical edge and reduce timely decision-making.

Desired Capabilities & Innovation Areas: Offerors have wide latitude to propose open-architecture software frameworks, distributed processing algorithms, or edge-native analytics across the following focus areas:

- Dynamic EMS Visualization: Intuitive, multi-echelon user interfaces and visual rendering engines that translate complex, high-density RF signal environments into simplified, real-time spatial and temporal visualization layers. Solutions should provide automated change detection, anomaly identification, and contextual RF overlays that allow operators, intelligence analysts, and commanders to immediately discern situational changes and contested spectrum sectors without parsing raw waveform data.
- Automated Non-Lethal Battle Damage Assessment (NL-BDA): Algorithmic automation and decision-support engines capable of autonomously measuring, quantifying, and validating the efficacy of deployed electronic attack and non-lethal spectrum effects against intended target signatures. Proposed solutions should correlate post-strike RF measurements against pre-engagement baselines to tell operator whether non-lethal effects achieved the intended result.
- Edge-Native Analytics & Constrained Data Dissemination: Solutions should leverage edge-processing microservices, intelligent feature extraction, and prioritized data-filtering protocols designed to operate within DDIL constraints. Architectures should execute

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

heavy data processing locally at the sensor node, transmitting only lightweight, critical updates to minimize tactical bandwidth consumption and preserve low-latency responsiveness.

- Sensor-to-Shooter Integration: Open-architecture software plugins and APIs enabling seamless data synchronization between enterprise intelligence pipelines, edge nodes, and standard tactical architectures. Solutions must support direct integration into sensor-to-shooter workflows and establish bidirectional compatibility with next-generation mission command software.

Capability 4: Electromagnetic Attack & Active Countermeasures

Problem Statement: Modern multi-domain operations require scalable, distributed Electronic Attack (EA) and Counter-C5ISR capabilities to deny, degrade, disrupt, or deceive adversary electromagnetic and cyberspace dependencies across depth. Current EA architecture lacks the flexibility to transition between close-proximity tactical denial and long-range operational standoff, creating gaps in fires synchronization and exposing friendly formations to counter-detection.

Across Battalion (close-contact/maneuver), Brigade (tactical area of influence), Division (extended shaping), and Corps (deep-sensing/long-range standoff) echelons, tactical commanders require open, scalable, and adaptable EA frameworks capable of neutralizing adversary command and control (C2), multi-spectral sensors, weapon datalinks, and autonomous targeting networks without inducing friendly spectrum fratricide. Field training and soldier feedback have shown that many current or proposed systems remain difficult to integrate, too complex for non-specialist operators, and too dependent on contractor support for routine sustainment.

Desired Capabilities & Innovation Areas: Offerors have wide latitude to propose modular hardware-software architectures, cognitive EA algorithms, or distributed cooperative jamming techniques across the following focus areas:

- Platform-Tailored SWaP-C Scalability: Proposed solutions must be optimized for Optimized Size, Weight, Power, and Cost (SWaP-C) integration for dismounted and static operations and/or mounted on tactical vehicles and robotic ground and UAS platform. Proposed solutions must scale power and gain to deliver precise close-proximity effects and high-power, long-range standoff degradation.
- Cognitive Jamming & Remote Threat Engagement: Closed-loop algorithmic architectures capable of transitioning from operator-directed tasking to autonomous, real-time threat response. Solutions should support machine-speed reactive triggers (e.g., sense-and-jam, jam-on-energy, adaptive protocol disruption) and cognitive learning algorithms capable of identifying and countering novel, frequency-agile, or software-defined adversary waveforms in dense EMS environments.
- Broadband Multi-Threat Defeat: Advanced waveform generation techniques—including wideband Digital Radio Frequency Memory (DRFM), precise packet/protocol injection, synthetic target generation, and Navigation Warfare (NAVWAR / GNSS) denial/deception. Solutions must demonstrate verified efficacy against tactical military transceivers, commercial/military radar, and Group 1–3 UAS C2 and video datalinks, utilizing directional power control and dynamic sector-blanking to protect friendly communications.
- Distributed Cooperative EA & Joint Fires Integration: Networked, multi-node

The Army FUZE xTech Program – G-TEAD USAREUR-AF ACE 27-02 Spectrum Enabled Warfare Powered by xTech Competition Announcement

algorithms that orchestrate synchronized, multi-platform jamming vectors to achieve spatial power combining, continuous target engagement during platform handoffs, and multi-angle signal injection. Architectures must natively synchronize with next-generation mission command software, EW and electromagnetic spectrum operations command-and-control software, and theater fires networks to seamlessly integrate non-lethal effects into lethal sensor-to-shooter targeting chains.

APPENDIX B: EFDI Data Backbone Vendor Integration — Call to Industry

Audience: prospective vendors and integrators responding to this call to industry. **Purpose:** to orient a Vendor to the EFDI Data Backbone architecture and to state, in advance of award, the interface obligations a Vendor system must satisfy to exchange data over it. Compliance with the requirements in Part 2 is a **condition of procurement**. A system that does not meet Requirement 4 cannot connect, and a system that does not meet Requirements 1 and 2 cannot publish or subscribe.

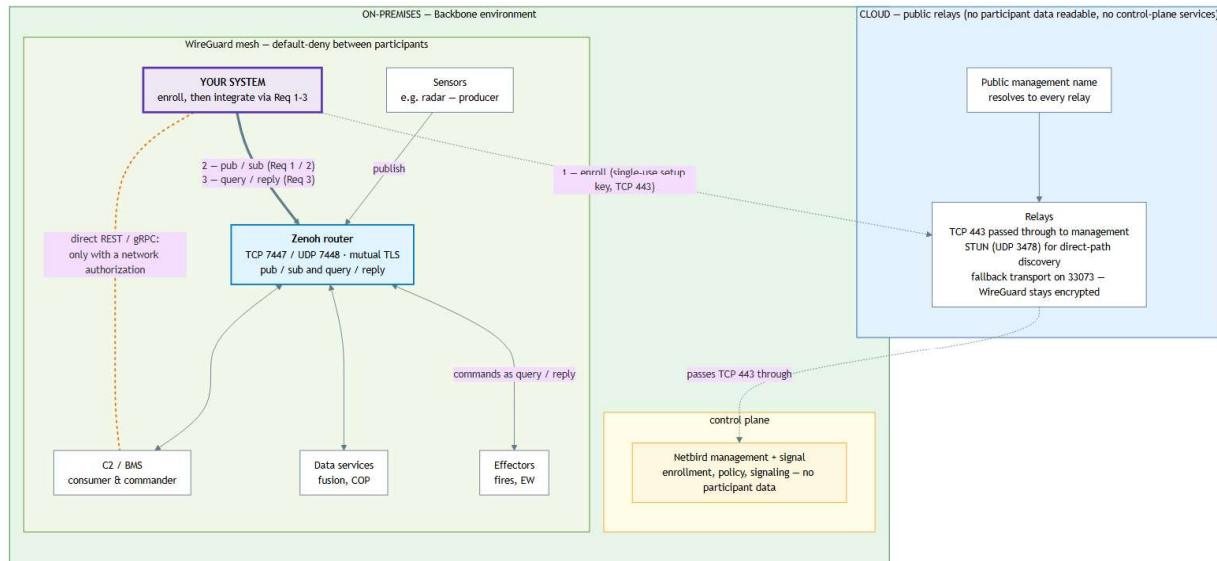
Currency: the facts in this paper were checked against the deployed configuration on 2026-10-01.

Defined terms

Term	Definition
EFDI Data Backbone ("the Backbone")	The open-architecture data fabric in use for NATO on the Eastern Flank under the Eastern Flank Deterrence Initiative (EFDI). It is the designated means of data exchange among participating systems.
Integration Gateway	The Backbone environment where a Vendor integrates before it operates. It is persistent: the interface a Vendor builds here is the interface it uses in operation.
Operational environment	The Backbone environment where the mission runs. It is a separate network from the Integration Gateway, with its own enrollment keys and its own certificate authority.
Event-driven data	Continuously or asynchronously emitted observational data — for example, radar tracks, sensor detections, and position reports.
Control command	A discrete, addressed, request/response action — for example, an engage order, a mode or state change, or a tasking message.
Zenoh	The designated open publish/subscribe and query/reply protocol for data on the Backbone. Each environment runs a Zenoh router ; Vendor systems connect to it as clients . The router routes; it is not a message broker and provides no central queue or dead-letter queue.
Netbird	The designated mesh enrollment and control service, layered over WireGuard. It provides the encrypted overlay network that every system joins.
Namespace	The part of the Zenoh keyspace one identity owns. Each person and each machine is issued its own, identified by a 32-character identifier, and only that identity can publish under it.
Fabric credential	The X.509 client certificate, private key, and environment root certificate a participant uses to authenticate to the Zenoh router. The certificate names the holder's namespace.
Setup key	A single-use key, issued per device, with which a system enrolls in the mesh.
Colorless transport	Bearer-agnostic connectivity in which the underlying link carries only opaque, encrypted packets and is indifferent to the data's classification, source, or content.

Part 1 — What You Are Integrating Into

This part is a short orientation to the Backbone architecture, so a Vendor can see where its system connects before reading the interface obligations in Part 2.



The layers

The Backbone has two layers, and a Vendor system joins both: an encrypted mesh network, and a data fabric that runs inside it.

The mesh. Every system enrolls as a peer in a WireGuard overlay network managed by Netbird. The overlay runs over any bearer — internet, satellite, cellular — and shows that bearer only encrypted packets.

- **Reach is default-deny.** An enrolled Vendor system can reach the environment's shared services and nothing else: the Zenoh router (TCP 7447, UDP 7448), mesh DNS (53, 5353), and web services (TCP 443). It has **no network path to another participant's system** unless a specific, time-bounded authorization opens one.
- **Traffic takes a direct path when one exists.** Two peers that can reach each other exchange WireGuard packets device-to-device. When a direct path cannot be established, the same encrypted packets go through a relay.

The data fabric. Each environment runs a Zenoh router on the mesh. A Vendor system connects to it as a Zenoh client over mutual TLS, using its fabric credential, and publishes and subscribes by key expression. Event-driven data and control commands both travel this way.

The cloud relays

A small set of cloud relays is the only part of the Backbone with public addresses. They do three jobs and can read no participant data in any of them.

- **Public entry.** The environment's management name resolves to the relays. A relay passes TCP 443 through to the management service without terminating TLS.
- **Path discovery.** The relays answer STUN requests (UDP 3478) so two peers can find a direct path through NAT.
- **Fallback transport.** When no direct path exists, a relay forwards peers' WireGuard packets on port 33073 (TCP as WebSocket over TLS, UDP as QUIC). The relay terminates its own transport session; the WireGuard packets inside remain encrypted end to end between the two peers.

The management service

The Netbird management and signal services run on on-premises hardware, not in the cloud. A Vendor system contacts them through the relays.

- An enrolled system holds one long-lived connection to management on TCP 443. It carries enrollment, policy updates, and the signaling used to set up peer connections.
- Management carries no participant data.
- Connections already established keep working if management becomes unreachable. New connections and policy changes wait until it returns.

Where your system connects

A Vendor system connects by three numbered paths, the same in both environments:

1. **Enroll as a mesh peer** (baseline precondition, Requirement 4).
2. **Exchange event-driven data through the Zenoh fabric** — **publish** if your system produces it (e.g., radar tracks), **subscribe** if it consumes it (e.g., a C2 system). Publishing is bound to your identity (Requirements 1 and 2).
3. **Exchange control commands as request/response** — discrete commands (e.g., an engage order or a state change) are carried through the fabric as Zenoh query/reply. A direct REST or gRPC connection between two systems requires its own network authorization (Requirement 3).

A single system commonly uses more than one path: in the diagram, a C2 system **subscribes** to tracks (path 2) and **issues** engage orders (path 3).

Two environments, one interface

The Integration Gateway and the operational environment present the same interface and the same enrollment procedure. What differs is the credentials.

- **Same procedure.** In both, a system enrolls against a public management name over TCP 443 with a single-use setup key, then connects to that environment's Zenoh router with a fabric credential.
- **Separate credentials.** Each environment has its own setup keys and its own certificate authority. A setup key or fabric credential issued for one environment is not accepted by the other.
- **Integration carries over.** Requirements 1 through 4 are identical in both environments, so work done on the Integration Gateway is not repeated to go operational.

How a Vendor is onboarded

Onboarding issues two things to each person and each machine: a setup key for the mesh and a fabric credential for the data fabric.

1. **People.** A sponsor already on the Backbone issues a one-time invitation. The Vendor's representative completes the intake form, which records their organization and nationality. The sponsor and then an administrator approve the application.
2. **Credentials.** On approval the representative receives a setup key for their device and a fabric credential. The credential package contains the client certificate and key, the environment root certificate, and a working first-publisher and first-subscriber example.
3. **Machines.** An approved representative enrolls the Vendor's machines against a quota that a Backbone operator sets. Each machine receives its own single-use setup key, its own namespace, and its own fabric credential. A radar gateway and a C2 server are two machines with two identities.
4. **Catalog.** The Vendor registers each topic it publishes, with its schema, in the Backbone portal's catalog. The catalog is how other participants find what exists and how to decode it.

What your network must allow

A system behind a corporate firewall needs outbound rules only. Nothing on the Backbone connects inward to a Vendor network.

Destination	Port	Protocol	Carries	Needed
Management name (resolves to the relays)	443	TCP	Enrollment, then one long-lived HTTP/2 stream	Required
Every relay	33073	TCP	Relayed traffic, WebSocket over TLS	Required
Every relay	33073	UDP	Relayed traffic, QUIC	Strongly recommended
Every relay	3478	UDP	STUN, direct-path discovery	Recommended
Other participants' public addresses	Various	UDP	Direct WireGuard, device-to-device	Optional

- **Allow every relay, not a subset.** A partial list breaks some peer pairs and not others.
- **Exempt these addresses from TLS inspection** and from short idle timeouts. The management connection is held open and quiet by design.
- **The address list for each environment** is published on that environment's onboarding guide and is provided at onboarding.

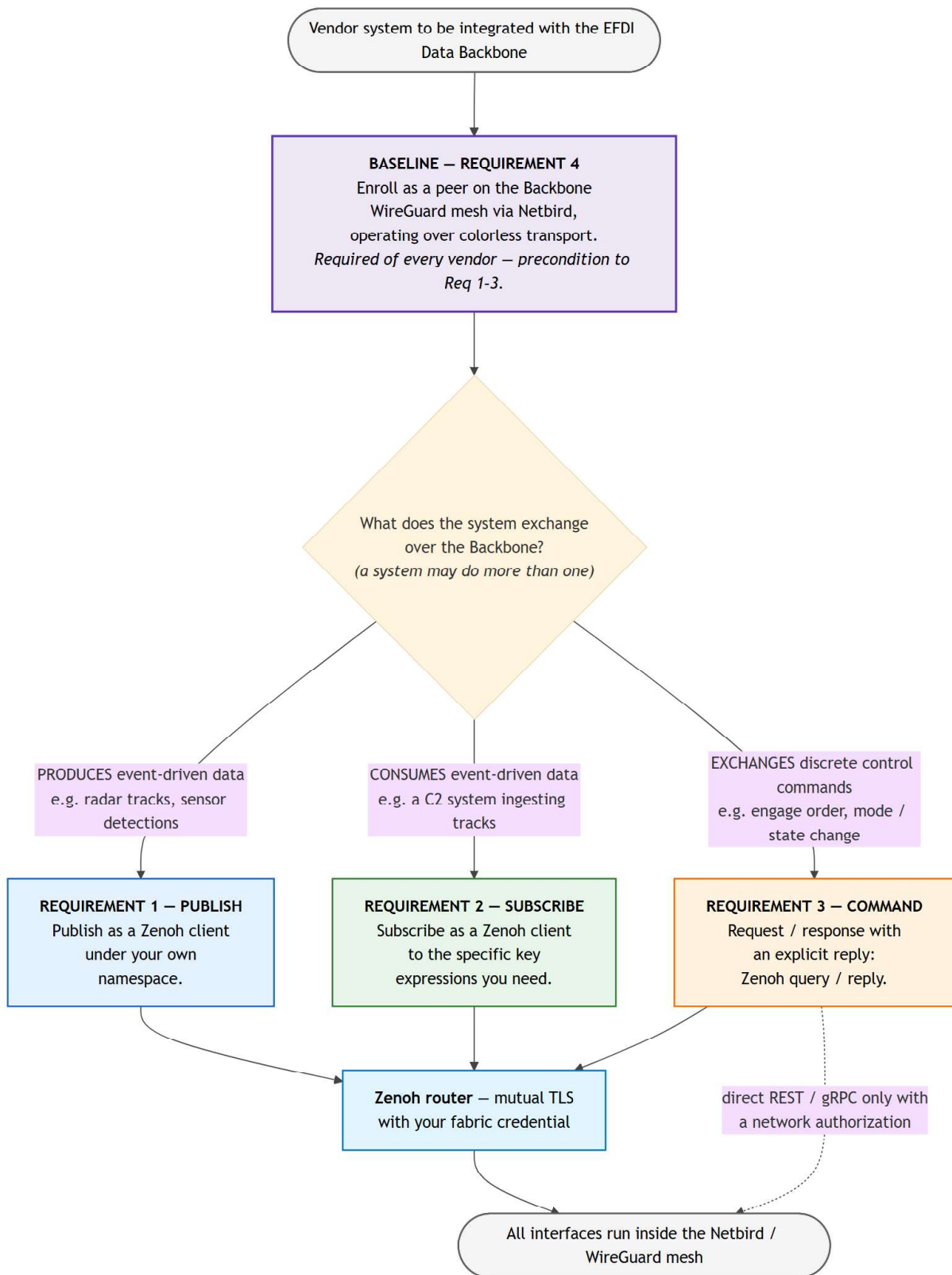
What stays under your control

- Your system runs **standard WireGuard** on the mesh; relays cannot read your traffic.
 - Only your identity can publish under **your namespace**.
 - Your internal implementation behind your system's edge is yours — the Backbone specifies the interface at the boundary, not your internals.
-

Part 2 — Interface Requirements

Decision diagram

The following diagram determines which interface obligation(s) apply to a given Vendor system. A single system may fall into more than one branch (for example, a Command-and-Control system that **consumes** event-driven tracks under Requirement 2 and also **issues** engage orders under Requirement 3).



Interface requirements

Requirement 4 (Baseline) — Mesh connectivity

Every Vendor system **shall** be capable of enrolling as a peer in the Backbone's WireGuard mesh network via the designated mesh control service (**Netbird**), operating over **colorless transport**. Enrollment is a precondition to Requirements 1 through 3.

- The system **shall** enroll with the standard Netbird client, a Backbone-issued single-use setup key, and the environment's public management name over TCP 443.
- The system **shall** operate with outbound connectivity only, as listed in Part 1 under "What your network must allow".
- The system **shall not** depend on a network path to any other participant's system. Enrollment grants reach to the environment's shared services only.

Requirement 1 — Event-driven producers shall publish

Any Vendor system that **produces** event-driven data (e.g., radar tracks, sensor detections) **shall** publish that data to the Backbone over **Zenoh**, under its own organization namespace, authenticated by its Backbone-issued fabric credential.

- The system **shall** connect to the environment's Zenoh router in **client mode** over mutual TLS. It **shall not** join as a router or peer.
- The system **shall** be wire-compatible with Zenoh 1.9.0, the version the Backbone runs.
- The system **shall** publish only under its own namespace. A publication outside that namespace is dropped by the router, and no error is returned to the publisher; a Vendor verifies delivery by reading the data back.
- Each topic **shall** carry exactly one message type, and the Vendor **shall** register the topic and its schema (a Protocol Buffers descriptor or an XML schema) in the Backbone catalog.
- The Vendor **shall not** retain the canonical copy of such data in a vendor-proprietary store reachable only through a vendor-operated portal or API.

A system that cannot embed a Zenoh client library may publish through the Backbone's HTTP-to-Zenoh publish bridge. The Vendor runs the bridge beside its application with the system's own fabric credential. The bridge publishes only; it does not subscribe.

Requirement 2 — Event-driven consumers shall subscribe

Any Vendor system that **consumes** event-driven data (e.g., a Command-and-Control system ingesting tracks) **shall** receive that data by subscribing to the applicable Backbone topic(s) over **Zenoh**, as a client authenticated by its Backbone-issued fabric credential.

- The system **shall** subscribe to the specific key expressions it needs. It **shall not** subscribe to, query, or store the entire keyspace.
- Read access follows the data owner's release decision. Data an owner has not restricted is readable by every authenticated participant. Data an owner has restricted is readable only by identities the Backbone operator has granted, and the Vendor requests that grant per integration.

Requirement 3 — Control commands shall use request/response

Any Vendor system that **issues or receives** discrete, non-event-driven control commands (e.g., engage order, mode or state change, tasking) **shall** do so as a request/response interaction with an explicit reply, not as an unacknowledged publication.

- **Default carrier: Zenoh query/reply.** The receiving system declares a queryable under its own namespace, and the issuing system queries it. The command travels over the same authenticated client connection as Requirements 1 and 2 and needs no additional network path.
- **Direct REST or gRPC, by exception.** A point-to-point REST API or gRPC service between two systems is permitted where a specific integration justifies it. Because enrolled systems have no network path to each other by default, it requires a Backbone network authorization naming the source, the destination, the ports, an owner, and an expiry date.
- **Command authority.** Which identities may command a given system is decided per integration with the Backbone operator and the owner of the commanded system.

At-a-glance mapping

If your system...	Example	Required interface	Technology
Produces event-driven data	Radar emitting tracks	Publish	Zenoh client (pub/sub)
Consumes event-driven data	C2 ingesting tracks	Subscribe	Zenoh client (pub/sub)
Exchanges control commands	Engage order, state change	Request/response	Zenoh query/reply; REST or gRPC by authorized exception
Any of the above	All vendors	Mesh peer enrollment	Netbird / WireGuard

Rationale (informative)

- **Why pub/sub for event-driven data.** Event-driven producers do not know — and should not need to know — every downstream consumer. Publishing to a named topic decouples producers from consumers and eliminates point-to-point N×N integration between systems.
- **Why request/response for control commands.** A discrete command needs a synchronous acknowledgment: the issuer must learn whether it was accepted. A query with a reply gives that; an unacknowledged publication does not.
- **Why commands go through the fabric by default.** A direct connection between two systems is a network path that must be authorized, reviewed, and expired for every pair. Carrying commands as Zenoh query/reply uses the one identity and the one connection a system already has, so adding a commanded system does not add a network path.
- **Why a mesh baseline.** Every system is reachable by identity over any bearer, and the bearer sees only encrypted packets — the colorless-transport property. Because management carries no participant data, connections between systems outlast a loss of the management service.