I. Background and Purpose

The U.S. Army is seeking innovative solutions from eligible entities, including but not limited to students, independent developers, startups, engineers, large technology companies and academic researchers across the globe addressing identified capability gaps in alignment with the objectives of the xTech National Security Hackathon. This platform offers opportunities to engage directly with Department of War (DoW) stakeholders, gain insights into Army and DoW problem sets and rapidly develop novel concepts aligned with Army and DoW priorities. Participants will have the opportunity to compete for prize awards and may have opportunities to pursue further development of their solutions for potential transition into Army applications following the event.

The Army FUZE xTech Program is partnering with U.S. Navy, U.S. Space Force, Cerebral Valley and Shield Capital to deliver the xTech National Security Hackathon. Additional partners for this effort may include: OpenAI, Scale AI, In-Q-Tel, DCVC, Armada AI, Deloitte, TENEX, Palantir and Skyrun. Unlike traditional solicitations, this initiative is structured as a time-bound innovation event in which participants will ideate, design and prototype solutions during the hackathon itself, rather than submitting fully developed technologies in advance.

The xTech National Security Hackathon will consist of one (1) round with two (2) parts:

(1) Registration application; and
(2) Hackathon event.

The U.S. Army intends to award up to $50,000 in cash prizes for the Hackathon to selected participants. Up to 700 applicants will be invited to participate in the hackathon event. The U.S. Army intends to select up **five (5) winners** at the conclusion of the hackathon event. Prize awards may be distributed as follows: first place may receive $20,000; second place may receive $12,000; third place may receive $8,000; fourth place may receive $6,000; and fifth place may receive $4,000.

Additional details on prize structure can be found in Section VII.

The xTech National Security Hackathon 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 – Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs

Government organizations are encouraged to 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 xTech National Security Hackathon may generate interest by other U.S. Army, DoW or 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.

The xTech Program intends to provide feedback from evaluators to participants during the hackathon competition event. 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

Eligible participants include, but are not limited to, students, independent developers, startups, engineers, large technology companies, and academic researchers across the globe. Both U.S.-based and international individuals and entities may participate, subject to the conditions below.

Each eligible entity:

- Shall not be a U.S. Federal 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 to the Government for work described in the problem statement;
- For businesses, startups and sole proprietors, must be able to obtain a CAGE code (U.S. businesses) and/or NCAGE code (international businesses) to process payments (CAGE codes are not required during registration);
- Applicants must be 18 years or older by the registration deadlines of May 2, 2026;
- Must not be based in a foreign country of concern (FCOC), directly funded by an FCOC-government or FCOC-government-subsidized guidance fund or be under the influence of an FCOC-based government in any way. Failure to meet these requirements will result in ineligibility for award;
- For all other eligible participants (including, but not limited to, independent developers, engineers, academic researchers, and large organizations): must be legally authorized to participate in the competition, and receive payments or awards in accordance with applicable laws and regulations;
- Shall be at the sole discretion of the Government; and
- Participants will be required to pass a Due Diligence check performed by the U.S. Army.

III. Topics and Problem Statement

U.S. Army operational units, in coordination with the broader DoW, are increasingly challenged

by adversaries employing widely available, low-cost technologies, including unmanned systems and electronic warfare capabilities. These threats are rapidly evolving and can be deployed at scale, creating complex and contested operational environments. At the same time, existing systems may present limitations in terms of cost, scalability, deployment speed, and operational flexibility, particularly for distributed and forward-positioned units.

To address these challenges, the U.S. Army, on behalf of DoW stakeholders, is seeking innovative, practical, and scalable solutions that can enhance mission effectiveness across a range of operational contexts. Of particular interest are approaches that improve sensor integration and analysis, enable resilient edge-based operations, enhance mission command and control, strengthen digital defense and cybersecurity capabilities, and address broader national security needs.

The Army is interested in concepts that are adaptable to resource-constrained environments, support distributed operations, and can be developed and transitioned in alignment with DoW priorities and applicable requirements. Collaboration with a broad range of participants, including commercial industry, academia, and independent developers, is encouraged to accelerate the development of relevant capabilities.

The Army intends to evaluate proposed solutions across the following capability areas:

- Capability 1: Sensor Analysis and Integration
- Capability 2: Edge Deployments and Drone Operation
- Capability 3: Mission Command and Control
- Capability 4: Digital Defense and Cybersecurity
- Capability 5: General National Security

For details on the full capability areas, see Appendix A.

IV. Program Submission

The xTech National Security Hackathon is voluntary and open to all entities that meet eligibility requirements listed in Section II (Eligibility Requirements). **Each individual or team may submit only one (1) application.**

The registration information and submission upload must be received by **9:00 AM PT on May 2, 2026.** Submissions received after the deadline will not be considered.

All submissions will be evaluated by a panel composed of representatives from the Army, DoW, and external stakeholders.

Register by selecting the xTech National Security Hackathon image at:
https://www.xtech.army.mil/

V. xTech National Security Hackathon Structure

Registration

All eligible entities must apply **using the Cerebral Valley Registration Form.** The application requires completion of a short questionnaire, which includes the following items:

1. LinkedIn profile
2. GitHub profile

3. Twitter/X handle (if applicable)
4. Description of the project you intend to develop at the hackathon
5. A defense-related project you are most proud of building
6. Home nationality and U.S. citizenship status (required for all applicants)

This information is collected to evaluate participants' technical aptitude and suitability for addressing the capability areas outlined in this RFI. The Army reserves the right to modify or supplement these questions as necessary.

The registration window will open **April 14, 2026**, and close **May 2, 2026, at 9:00 AM PT**. Applications will be reviewed on a **first-come, first-served basis**, and applicants may be notified of their selection as submissions are received. Selection for the hackathon is at the **sole discretion of the U.S. Army and participating partner organizations**. While applicants may believe their concepts align with the stated topic, final determinations will be made exclusively based on the content, clarity, and relevance of the information provided in the registration form and its alignment with Army and DoW priorities as defined in this announcement.

Up to **700 applicants** will be selected and invited to participate in the hackathon, which will take place **May 2-3, 2026**.

Hackathon Event

Selected applicants from the registration process will participate in a **two (2)-day hackathon event**, where they may collaborate as individuals or in teams to develop innovative solutions addressing the capability areas outlined in this RFI. During the event, participants will **design, build, and demonstrate working prototypes or concepts**, emphasizing technical quality, operational relevance to the U.S. Military, and creative problem-solving. Participants will also **present and pitch their solutions to a panel of subject matter experts**, highlighting both the functionality and the potential impact of their work.

The event is currently scheduled to take place **Saturday, May 2, 2026, beginning at 9:00 AM PT, and concluding on Sunday, May 3, 2026, at 5:00 PM PT**, at **SHACK 15 in San Francisco, California**. **Additional details, including exact agenda and logistical instructions, will be provided to selected participants prior to the event.**

Each individual or team will be evaluated based on the following evaluation criteria:

Criterion	Weight
Technical Demo How is the demo? Is the project implemented technically well? Is it well-engineered and working?	35%
Military Impact Potential Does the project address a significant real-world issue or pain point for the US Military?	30%
Solution Creativity How creative is the project? Have you seen this before? Does it solve the problem in a novel or unique way?	25%
Presentation & Pitch How well was the project presented and demonstrated to stakeholders?	10%

Tentative Hackathon Event Schedule:

Date	Time	Activity
Saturday, May 2, 2026	9:00 AM PT	Doors Open for Hackers + Team Formation
	11:00 AM PT	Welcome Kick-off + Presentation
	11:45 AM – 10:00 PM PT	Hacking Starts – Lunch and dinner will be served. *Doors close at 10:00 PM PT *(Hackers may stay overnight, but no reentry is allowed)*
Sunday, May 3, 2026	9:00 AM PT	Doors Open for Hackers + Team Formation
	12:00 PM PT	Hacking Stops & Submissions are Due
	12:00 PM PT	First Round Judge Briefing & Huddle
	12:15 – 2:00 PM PT	First Round Judging – Lunch will be served at 1:00 PM PT
	2:10 PM PT	Finalists Announced & Demos Begin for Final Judging Round
	2:45 PM PT	Final Round Judge Deliberation
	3:15 PM PT	Winners Announced & Closing

Dates and times are subject to change.

Upon conclusion of the hackathon on Sunday, May 3, 2026, the xTech Program will select **up to five (5) final winners.** Prize awards may be distributed as follows: **first place may receive $20,000; second place may receive $12,000; third place may receive $8,000; fourth place may receive $6,000; and fifth place may receive $4,000.**

VI. Proposed Schedule

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

Date	Activity
April 14– May 2, 2026	Registration open on a rolling basis
May 2-3, 2026	Hackathon Event at SHACK 15
May 3, 2026	Winners announced at 3:15 PM PT

VII. Prizes and Incentives

Prizes will be offered under 10 U.S.C. §4025 (Prize Competitions). The total prize pool is $50,000. Other non-monetary incentives are provided through the xTech National Security Hackathon to help industry engage with the U.S. Army.

Phase	Winners	Prize
Registration	Up to 700	Entry into the Hackathon
Hackathon Event	Up to five (5) final winners	1st place: $20,000 2nd place: $12,000

Phase	Winners	Prize
		3rd place: $8,000 4th place: $6,000 5th place: $4,000
	Total	$50,000

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 intellectual property (IP) rights and management by the private sector and DoW.

For the xTech National Security Hackathon 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 Hackathon 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 Hackathon 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 by selecting the xTech National Security Hackathon image 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/

APPENDIX A – Problem Statement Descriptions

Problem Statement 1: Sensor Analysis and Integration

Modern operations depend on fusing data from many sensor types, including EO, IR, RF, radar, and more into a single actionable picture. How can we consolidate detections across modalities, optimize sensor search strategies, and maintain custody of targets in contested environments?

Example Projects:

- Develop an algorithm that optimizes sensor search strategies across multiple sensor types to maximize the probability of reacquiring a lost target while minimizing search time, accounting for the target's last known state, maneuverability, and sensor constraints
- Build a system that automatically fuses multiple detection messages from different sensors into a single correlated event, iteratively refining confidence, estimated time, and location as new data arrives
- Create a processing pipeline that analyzes uncorrelated tracks to identify candidate paths of objects that may be actively evading detection, distinguishing between debris, separations, and potential threats

Problem Statement 2: Edge Deployments and Drone Operation

Operators on the front lines need to command autonomous systems from austere, disconnected environments, sometimes from nothing more than a backpack. How can we push computation and control to the tactical edge and build resilient drone systems, all while balancing power, latency, and mission complexity?

Example Projects:

- Design a lightweight edge computing architecture capable of running drone command-and-control and onboard inference from a portable, battery-powered kit optimized for field conditions
- Build a system that enables a single operator to task and coordinate a small swarm of autonomous vehicles from an edge device, even when connectivity to a central network is intermittent or denied
- Develop a real-time sensor processing pipeline deployable on edge hardware that ingests video and RF data from drones, performs local target detection, and pushes prioritized alerts without reliance on cloud infrastructure

Problem Statement 3: Mission Command and Control

Command and control means synthesizing information from across the battlespace into a coherent picture and acting on it faster than the adversary. How can we integrate sensor feeds, intelligence, and unit positions into a unified interface that accelerates the kill chain and decision-making?

Example Projects:

- Build a battlefield command dashboard that integrates live feeds from multiple data sources (sensor tracks, unit positions, vehicle locations, communications, intelligence reports) into a unified operational picture with intuitive visualization and natural language querying
- Develop a system that automates key steps in the kill chain, from detection through identification to engagement recommendation, while maintaining human-in-the-loop oversight and explainable rationale

- Create a tool that ingests operational reports, automatically links entities (people, units, locations, events, etc.) into a knowledge graph, and surfaces emerging patterns or threats to command staff in real time

Problem Statement 4: Digital Defense and Cybersecurity
As military and AI systems become more networked and software-defined, they become prime targets, as we've seen recently with an increased frequency of hacks, leaks, and supply chain attacks. How can we automatically detect and mitigate attacks on mission-critical infrastructure, protect AI deployments and communications links, and harden the digital backbone that modern operations depend on?
Example Projects:

- Develop an automated system that detects and mitigates distributed denial-of-service attacks on ground-based sensor and communication assets, maintaining mission continuity during active cyber engagement
- Build a monitoring and anomaly detection pipeline that identifies unexpected changes in RF transmissions, such as shifts in frequency, power, or modulation, that may indicate tampering or unauthorized changes in operational status
- Create a deployable security scanning toolkit that validates containerized AI model deployments against known-good baselines, detecting anomalous files, tampered libraries, or embedded threats before models influence operational decisions

Problem Statement 5: General National Security
After reading the above problem statements, what other ideas do you have to build for the benefit of national security? If you pursue this track, please speak with a mentor about your idea before you begin building to ensure it's a good fit. We'll have folks walking around to chat!