EMERGING TECHNOLOGIES INSTITUTE | NDIA

Competing for Capability:

Aligning Hackathons with Defense Acquisition Pathways

Ida Bagus Made Widyadnya,
Dr. Arun Seraphin, & Culley Horne

ETI Brief Series

April 2026

Authors

Ida Bagus Made Widyadnya, Dr. Arun Seraphin, & Culley Horne

Production

Zachariah Chou
Copywriter & Editor, NDIA

Eve Dorris
Director, IPO, NDIA

Alexander Feeser
Creative Director, NDIA

Vince Lim
Graphic Designer, NDIA

NDIA ETI Executive Director

Dr. Arun Seraphin

First published in April 2026 by NDIA's affiliate, the Emerging Technologies Institute.
2101 Wilson Blvd, Suite 700, Arlington, VA 22201,
United States of America. (703) 522-1820.

This report is made possible by general support to NDIA and the Emerging Technologies Institute. No direct sponsorship contributed to this report. This report is produced by NDIA, a non-partisan, non-profit, educational association that has been designated by the IRS as a 501(c)(3) nonprofit organization and was founded to educate its constituencies on all aspects of national security. Its research is nonpartisan.

For more information please visit our website: EmergingTechnologiesInstitute.org

MEDIA QUERIES: Rachel Sutherland, NDIA Director of Public Affairs & Communications at rsutherland@NDIA.org

Executive Summary

Hackathons and other structured technical events (code sprints, Red/Blue Team Exercises, Prototyping Challenges) are playing a growing role in the Department of Defense (DoD)'s approach to rapid problem-solving and early-stage technology development. These events frequently generate promising prototypes, practical technical insights, and new modes of engagement with industry and the broader defense innovation community. Yet hackathons and similar initiatives remain only loosely linked to the Department's formal acquisition and fielding pathways. As a result, even solutions that demonstrate clear operational relevance often stall at the proof-of-concept stage, lacking a reliable mechanism to transition to sustained experimentation, structured prototyping, or programs of record. A recurring concern is that the core legal framework needed to support certain follow-on actions already exists under current authorities, and in some cases is already used in practice. The practical gap, however, is less the absence of legal authority and more the absence of repeatable implementation mechanisms, resourced transition planning, and program-aligned investment decisions that move promising hackathon outputs from event delivery to funded acquisition pathways.

This brief assesses the role hackathons currently play within the defense innovation ecosystem and identifies the structural and policy barriers that limit their ability to scale and transition. It reviews recent legislative developments, most notably the Defense Hackathon Act of 2024, to evaluate how Congress has sought to institutionalize hackathons while leaving core transition challenges largely unresolved. It also proposes targeted legislative language to amend Section 1503 of the FY2025 NDAA (Pub. L. 118-159).

Recommendations focus on (1) clarifying when and how federal prize authorities should apply to hackathon-generated solutions; (2) enabling appropriate follow-on contracting and experimentation without restarting duplicative competitive processes; (3) expanding access to secure, compliant development environments that reduce cybersecurity compliance friction; and (4) integrating acquisition and resource personnel into hackathon event designs so that viable work products may be paired with executable transition plans, identified contracting shops, and mapped funding sources capable of supporting follow-on prototyping and fielding.

Introduction

Hackathons have emerged over the past two decades as a prominent model for accelerated problem-solving in technology development. First documented in open-source communities in the late 1990s,[1] hackathons are short-duration, high-intensity innovation competitions that bring together diverse participants to develop practical solutions, test prototype concepts, and foster cross-team collaboration. Leading tech firms routinely use hackathons internally to spark innovation and home in on emerging standards and practices.[2] Hackathons aim to compress the conventional innovation cycle from months or years to mere days, enabling quick iteration and proof-of-concept demonstrations.[3] The hackathon model is increasingly embraced as a way to drive concrete outcomes by aligning participants with pressing problems under tight time constraints.

In recent years, there has been an increasing use of hackathons within the DoD as a mechanism to engage a broader pool of technical experts and allow them to support and accelerate the development of technical solutions that address persistent or emerging military operational shortfalls.[4] Well-designed hackathons bring together significant technical talent from defense and commercial industry, government organizations, and academia, along with end-users who have identified real-world use cases or problems to be addressed. When hackathon participants are provided with enough real or synthetic data alongside a clear understanding of real-world operational challenges or military requirements, and given a sense of practical, technical, and operational constraints, hackathons can yield useful solutions that can contribute to the Department's capability modernization efforts.[5]

When well-executed, a hackathon's two- to five-day sprint can produce a product at Technology Readiness Levels (TRL) one through three[6], potentially comparable to the proof-of-concept stage of a Small Business Innovation Research (SBIR) Phase I[7] or

1 Gerard Briscoe & Catherine Mulligan, Digital Innovation: The Hackathon Phenomenon, ***Queen Mary Univ. London*** & ***Imperial Coll. London***. (2014). https://qmro.qmul.ac.uk/xmlui/bitstream/handle/123456789/11418/Briscoe%20Digital%20Innovation:%20The%20Hackathon%20Phenomenon%202014%20Published.pdf?sequence=2

2 Charles Ott, Why hackathons are cracking the code on government innovation, Maximus. (Aug. 6, 2025). https://maximus.com/insights/hackathons-accelerate-federal-innovation

3 Derrick Pledger, Hackathons: A Strategic Tool in Defense Innovation, Nat'l Def. Mag. (Aug. 4, 2025). https://www.nationaldefensemagazine.org/articles/2025/8/4/hackathons-a-strategic-tool-in-defense-innovation

4 Jon Harper, Hackathon at Indo-Pacific Command's new AI battle lab open to all US citizens, DefenseScoop. (Dec. 7, 2023). https://defensescoop.com/2023/12/07/hackathon-at-indo-pacific-commands-new-ai-battle-lab-open-to-all-us-citizens/

5 Master Sgt. Zachary Vucic, AFCENT Battle Lab Hosts Hackathon 25.4, Seeking Innovative Solutions for Warfighting Challenges, Air Forces Central Public Affairs. (Sept. 26, 2025). https://www.afcent.af.mil/News/Article/4316180/afcent-battle-lab-hosts-hackathon-254-seeking-innovative-solutions-for-warfight/

6 Office of the Under Secretary of Defense for Research and Engineering, Technology Readiness Assessment Guidebook, Department of Defense. (Feb. 2025). https://www.cto.mil/wp-content/uploads/2025/03/TRA-Guide-Feb2025-Cleared.pdf

7 See 15 U.S.C. § 638.

RDT&E Budget Activity 1 (6.1)[8] basic research project. In addition to rapid tempo, hackathons serve as hubs for collaboration and learning where competitors share best practices and frequently converge on emerging platforms and standards. Furthermore, by lowering the barriers to entry for prototyping, hackathons can lead to greater overall innovative technology development activity between new technical partners and organizations.

Today, hackathons have demonstrated the ability to attract large groups of technical and operational experts to attempt the development and delivery of solutions. These activities are consistent with efforts to expand the defense industrial and innovation base, as well as the speed of delivery of technical products, even within the constraints of the limited time and resources typically dedicated to such efforts. In a few notable cases, similar structured technical competition models have already led to successful transitions into formal programs. For instance, the Army's xTechSearch 3 and AStRA competitions have helped solutions like the Dismounted PNT System Generation II (DAPS GEN II)[9] and Edge Processor-Aided Target Recognition (AiTR)[10] transition from winning projects to fielded programs of record. Such cases, unfortunately, remain the exception rather than the rule, as promising hackathon outputs often face a significant "last mile" integration gap. Understanding the nature and value of what hackathons can produce is key to closing this gap.

The NDIA Hackathon & IP Retention

At the National Defense Industrial Association (NDIA) 2025 *Emerging Technologies for Defense* Conference and Exhibition, NDIA hosted a global hackathon that brought together technology users and developers from industry, academia, and government. Participants worked in teams to address operational challenges identified by both government and industry organizations, including members of Combatant Commands such as U.S. INDOPACOM and EUCOM.[11]

Significantly, the NDIA hackathon also connected competitors with other operational users, technical experts, defense integrators, and industry representatives to inform the development of practical and effective solutions. Industry partners further contributed to the hackathon by providing computing platforms for use in the event. Hackathon participants were supplied with real-world operational data and other technical data related to systems performance and technical capabilities, made available by both government and industry sponsors.

The NDIA hackathon offers a useful case study of an industry-hosted model that is structured to reduce common transition frictions, especially around data access and intellectual property. This model, in which the intellectual property created during the event remains under the control of the companies (rather than transferring to the government), can help strengthen transition incentives of hackathon products into acquisition and operational use. Retaining ownership of IP increases incentives for companies to further develop and market their developed capabilities to a variety of government users and other interested industry partners.[12]

Hackathon Transition Pathways and Barriers

As a baseline, several legal pathways that could support hackathon-style competitions and initial awards already exist under current law.[13] Prize competition authority, in particular, is flexible in structure and can accommodate hackathon-style events. So long as a competition is structured to satisfy applicable competition requirements, agencies may be able to pursue follow-on actions consistent with existing acquisition authorities. Accordingly, the principal policy question is not whether hackathons can be run under existing authorities in isolated cases, but whether the Department has clear, repeatable mechanisms to connect event outputs to funded acquisition pathways.

Despite growing interest from technical experts, operational units, senior leaders, and both defense and commercial industry, hackathons have yet to transition outcomes consistently or at scale. Even where existing authorities can support prizes and certain follow-on actions, those authorities do not, standing alone, resolve the recurrent program-investment problem. Hackathon outputs frequently require a deliberate acquisition pathway, including identification of the appropriate contracting office, selection of the most suitable contracting instrument, alignment with an existing program line or transition sponsor, and a funding plan that is executable within fiscal law constraints.[14] Without

8 See DOD 7000.14-R, Vol. 2B.

9 Anna Volkwine, xTech Winner Delivers Program of Record Technology for GPS-Denied Soldiers, XTechSearch. (May 1, 2025). https://armysbir.army.mil/news/xtech-winner-delivers-program-of-record-technology-for-gps-denied-soldiers/

10 Jennie Jacobs, Toyon Wins Army xTech Competition with Edge Processor Aided Target Recognition Solution, Toyon Research Corp. (Oct. 1, 2021). https://www.toyon.com/news/press/toyon-wins-army-xtech-competition-with-edge-processor-aided-target-recognition-solution/

11 ETI Research Team, 8 Key Themes from NDIA's Emerging Technologies for Defense Conference 2025, NDIA ETI. (2025). https://www.emergingtechnologiesinstitute.org/publications/insights/2025etc-ro

12 Office of the Under Secretary of Defense for Acquisition and Sustainment, Intellectual Property Guidebook for DoD Acquisition, Department of Defense. (Apr. 30, 2025). https://www.acq.osd.mil/asda/dpc/api/docs/intellectual%20property%20guidebook%20for%20dod%20acquisition%20signed.pdf

13 See 10 U.S.C. § 4025 (a)–(b), (d), (f).; See also 15 U.S.C. § 3719 (b)–(f).

14 See 31 U.S.C. § 1301(a); 31 U.S.C. § 1502(a); 31 U.S.C. § 1341(a)(1).

these elements, hackathon outputs risk functioning as a one-time award mechanism rather than a repeatable transition mechanism.

External reviewers also noted a structural resource imbalance between the volume of industry-side transition effort that hackathons and other structured technical events can generate and the capacity of government offices that must execute the legal and administrative steps required for transition. Even where funding and contracting authorities exist, understaffing or limited specialist bandwidth (e.g., legal review capacity for IP and security-related documentation) can slow or block conversion of a hackathon output into a sustained acquisition action.[15] This current dynamic suggests that transition policy cannot be solely a matter of adding authorities, but also of ensuring that the Department has sufficient institutional capacity to execute the steps those authorities require.

One way to accelerate the transition of the technically useful and innovative products emerging from well-designed hackathons would be to adjust acquisition policy to streamline the process by which contractors engage for products and services. This could follow the model previously developed for technology prize authority (for instance, under 10 U.S.C. § 4025), which enables government organizations to award cash or other prizes to acknowledge and reward technology achievements through structured competitions. These prize authorities, first established under the FY 2000 NDAA[16] and later expanded through the America COMPETES Act,[17] have been used by DoD and other organizations for a wide variety of activities to support technological development and modernization missions. The Challenge.gov platform, managed by the General Services Administration, for example, has hosted over 2,000 prize competitions since 2010, producing solutions in fields ranging from healthcare to cybersecurity.[18]

Institutionalizing Hackathons Through Federal Prize Authority and Acquisition Reform

Recent legislation reflects policy support for leveraging hackathons to drive defense innovation. The Defense Hackathon Act of 2024, incorporated as Sec. 1503 of the FY 2025 NDAA,[19] directs the DoD to establish a formal "Hackathon Program". Under this initiative, the Department is tasked with conducting no fewer than four hackathons each year and developing common standards and infrastructure for the execution of these events. While this initiative attempts to institutionalize hackathons as a tool in the defense innovation ecosystem, additional policy measures are likely to be needed to ensure that hackathon-generated solutions can transition more effectively into the larger-scale defense acquisition process, prototypes, experiments, or acquisition programs of record for production and operational use.

Congress should consider explicitly recognizing well-designed hackathons, endorsed by senior operational or acquisition officials, as a form of technology prize competition under federal law. This formal codification would enable the DoD to make use of authorities under 10 U.S.C. § 4025 and award follow-on development prototyping or even production contracts to appropriate hackathon participants who have demonstrated delivery of useful solutions to identified operational challenges. In conjunction, policymakers could consider modifying selected sole-source justification authorities to account for technical achievements under hackathons and enhancing the authorities governing the use of follow-on contracting authority under SBIR, Other Transaction Agreements (OTAs), or prototyping language to pull successful projects into further stages of development or production.[20]

To preserve the intent of Sec. 1503 while increasing operational impact, Congress and the Department should also consider treating hackathons as dual-track events that incorporate both technical development and acquisition planning. In practice, this means ensuring participation by acquisition stakeholders, such as contracting officers and program representatives, in order to provide an acquisition and resourcing pathway capable of supporting follow-on execution on top of the production of technical solutions. This approach could be implemented synchronously within a single event, or serially through a linked sequence where a technical event is followed by an acquisition-focused planning sprint.

15 See National Industrial Security Program Operating Manual 32 C.F.R. Part 117; See also, DD Form 254.

16 See S.1059 Pub. L. No. 106–65, 113 Stat. 512

17 See H.R.2272 Pub. L. No. 110–69, 121 Stat. 572, 15 U.S.C. § 3719

18 Cristin Dorgelo, Scaling Effective Methods across Federal Agencies: Looking Back at the Expanded Use of Incentive Prizes between 2010-2020, Federation of American Scientists. (Aug. 29, 2024). https://fas.org/publication/government-incentive-prizes/

19 See H.R.5009 Pub. L. No. 118-159, § 1503, 138 Stat 2137.

20 See, e.g. 10 U.S.C. §§ 4004, 4021, 4022.

Secure Environments for Tech Integration

However, policy adjustments alone may not be sufficient to address integration challenges that consistently prevent the transition of promising hackathon outputs into operational use. A practical obstacle is often the security and compliance hurdle: technologies built within the span of several days may not align with federal cybersecurity requirements, making it hard to transition them into military networks or systems.[21] These challenges are particularly acute for software-enabled capabilities, where iterative development cycles, reliance on external libraries, and dependence on live or synthetic data streams complicate security accreditation and continuous authorization processes.[22]

A separate transition constraint identified by industry practitioners is the set of government-controlled prerequisite actions that industry cannot complete unilaterally, even when the technology is technically mature. These may include security classification specifications (DD Form 254) where classified work is contemplated, interconnection and data access arrangements for operating on government networks, and formal instruments documenting collaboration or funding relationships (for example, memoranda of understanding or memoranda of agreement, depending on the activity). Similarly, effective collaboration with government users often hinges on government-controlled identity and access requirements, including CAC sponsorship and related account provisioning.[23] Delays can create a practical bottleneck because these requirements are often necessary for secure collaboration, environment access, and, in some cases, contract execution.

A partial remedy could come in the form of a FedRAMP-authorized[24] or other pre-accredited development environment that allows hackathons to be conducted in compliance with government security requirements. Building solutions in an environment with an existing Authority to Operate (ATO) can likely reduce development overruns and shorten DoD Risk Management Framework (RMF) timelines,[25] thereby smoothing the difficult transition from a prototype (TRL 6) to an operational system (TRL 7), a phase often referred to as the "valley of death" for emerging technologies.[26]

Increased resources for security, compliance, and certification functions could allow the Department to better harness the benefits of hackathons, ultimately saving money and reducing technology risk for the Department. While current authorities allow sponsors to provide ATO-authorized or FedRAMP-compliant environments, the absence of explicit direction means it remains optional and uneven. Codifying this in law or the hackathon operating framework would elevate it from "permitted" to "expected," increasing adoption and making compliant environments a default part of hackathon execution.

Conclusion

Realizing the full potential of hackathons requires a full spectrum of institutional support across acquisition offices, security and certification stakeholders, operational commands, industry partners, and policymakers. To make outcomes repeatable, hackathons need stronger transition infrastructure: clear follow-on contracting pathways that move teams beyond proof-of-concept into prototyping, experimentation, or limited production; and Department-sponsored access to secure, compliant development environments that reduce cybersecurity and transition friction. Just as important, hackathon outputs must connect cleanly to existing defense acquisition authorities so that promising solutions do not stall post-event delivery. Finally, improving transition outcomes may require treating hackathons as an entry point to a broader investment-and-ordering ecosystem, using staged follow-on funding and a marketplace-style mechanism to match validated solutions with sponsoring programs and contracting organizations ready to place follow-on orders. At a time when the pace of technological development is critical to national security, empowering hackathons could improve the Department's ability to identify, test, and transition innovative capabilities, and ultimately deliver capable solutions to the hands of warfighters.

---

21 Defense Innovation Board, Scaling Nontraditional Defense Innovation, Department of Defense. (Jan. 8, 2025): 20. https://innovation.defense.gov/Portals/63/DIB%20Scaling%20Nontraditional%20Defense%20Innovation%20250113%20PUBLISHED.pdf#:~:text=network%20security%20for%20nontraditional%20vendors,such%20as%20the%20European%20Union

22 Department of Defense Chief Information Officer, Implementing the Continuous Authorization to Operate (cATO), Department of Defense. (2021). https://dodcio.defense.gov/Portals/0/Documents/Library/cATO-EvaluationCriteria.pdf?ver=A8tLIfPjmp3RpemU6JOhJw%3D%3D

23 For example, CAC issuance requires Defense Enrollment Eligibility Reporting System (DEERS) enrollment, and often hinges on related account provisioning (e.g., unclassified email) for access to government collaboration services.

24 See 44 U.S.C. § 3608

25 Atlassian, The Department of Defense's Platform One deploys Atlassian to provide modern DevSecOps services, Atlassian, (2021). https://www.atlassian.com/whitepapers/dod-devsecops-data-center

26 Committee on Accelerating Technology Transition, Accelerating Technology Transition: Bridging the Valley of Death for Materials and Processes in Defense Systems, National Research Council of the National Academies, National Academies of Sciences, Engineering, and Medicine. (2004). https://www.nationalacademies.org/read/11108/chapter/1

Possible NDAA Provision

SEC. [….] CLARIFICATION OF PRIZE COMPETITION ELIGIBILITY FOR HACKATHONS

Section 1503 of the Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025 (H.R.5009 Pub. L. No. 118-159, § 1503, 138 Stat 2137) is amended —

(1) by adding at the end, the following new subsections:

"(f) PRIZE AUTHORITY. — Hackathons conducted under the Program shall be considered competitions for purposes of section 4025 of title 10, United States Code, and the Department of Defense may award prizes to participants in such Hackathons in accordance with that section, provided that each hackathon uses competitive procedures consistent with the requirements of subsection (b) of such section.

"(g) FOLLOW-ON AWARDS. — The Secretary shall establish procedures to provide follow-on awards for research and development activities or procurement of products and services to participants in such hackathons.

"(1) Hackathons conducted under the Program shall be considered consistent with the definition of full and open competition as set forth in section 3201 of title 10, United States Code. Competitive procedures used in such hackathons executed consistently with criteria established under section 4025(b) of title 10 shall satisfy applicable requirements for full and open competition.

"(2) A follow-on award under subsection (g) may be made without additional justification and approval otherwise required by section 3204 of title 10, United States Code. The authority to award a follow-on contract or agreement to a hackathon winner under this subsection is authorized by law for purposes of the exception provided in section 3204(a) of this title."

Possible NDAA Committee Report Language

LEGISLATIVE PROVISIONS

SEC. [….]—Clarification of Prize Competition Eligibility for Hackathons

The committee recommends a provision that would amend Section 1503 of the Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025 (H.R.5009 Pub. L. No. 118-159, § 1503, 138 Stat 2137) to clarify that hackathons may qualify as competitions for purposes of awarding prizes under 10 U.S.C. § 4025, including prizes that may inform or initiate follow-on innovation programs such as Small Business Innovation Research awards. This clarification builds upon recent congressional efforts to institutionalize hackathons as part of the Department of Defense's innovation ecosystem.

The committee notes that structured technical events, such as hackathons, code sprints, red team/blue team exercises, and prototyping challenges, are increasingly employed by the Department to rapidly develop mission-relevant solutions in a collaborative, outcome-driven format. These events typically feature broad participation, clearly defined evaluation criteria, and tangible deliverables that inform capability development. However, the committee is concerned that ambiguity in existing statute may hinder the Department's ability to use prize authority to support post-award transition efforts and incentivize these activities.

Additionally, the committee observes that Congress has provided statutory flexibilities to promote innovation through alternative competition pathways. 10 U.S.C. 3204 permits certain non-competitive awards and explicitly waives justification-and-approval requirements for sole-source Phase III SBIR. Similarly, 10 U.S.C. 3201(e)(4) exempts contracts with the National Academy of Sciences from conventional competition requirements. The committee views these precedents as an affirmation of congressional intent to accommodate innovative procurement pathways within the defense acquisition framework.

The committee further encourages the Department to design hackathons and similar events to include appropriate acquisition, contracting, and resource personnel, with the objective of producing an executable transition plan, including identification of potential program sponsors, contracting pathways, and funding sources for follow-on efforts where warranted.

Therefore, the committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Acquisition and Sustainment, to provide a briefing to the congressional defense committees by [MM/DD/YYYY] on the Department's plan to implement this clarification. This briefing should detail how the Department will integrate prize authority into hackathons and similar events, ensure compliance with competition requirements, enable prize outcomes that support technology transition pathways, and maximize the impact of these events on technology transition and warfighter needs.

EMERGING TECHNOLOGIES INSTITUTE | NDIA

Supporting Emerging Technologies To Secure U.S. National Defense and Advance U.S. Economic Strength

The National Defense Industrial Association's Emerging Technologies Institute (ETI) performs research, hosts events, and bolsters public awareness through educational products and webinars focused on defense technology modernization and innovation. ETI also works to create a policy environment most conducive to the efficient development and delivery of new systems and technologies for the defense enterprise. ETI engages industry, academia, policymakers, and the public to explore emerging technologies' impact on national security and opportunities for industry-government partnerships to increase U.S. competitive advantage.

ETI reports, events, and workshops support NDIA's membership and the defense science & technology enterprise as part of its nonpartisan 501(c)(3) mission.

ETI was founded in 2021 and is staffed by researchers and subject matter experts and backed by a preeminent advisory board.

For more information, visit **EmergingTechnologiesInstitute.org**

EMERGING TECHNOLOGIES INSTITUTE
EmergingTechnologiesInstitute.org