DEFENSE INNOVATION BOARD

LOWERING BARRIERS TO INNOVATION

DIB | DEFENSE INNOVATION BOARD

innovation.defense.gov

Table of Contents

Preface

While the national defense innovation ecosystem is burgeoning with innovation efforts within and outside the Department of Defense, there still exist several internal barriers that prevent innovation from scaling at speed.

The Defense Innovation Board is chartered with the authority and responsibility to provide independent, practical, and actionable recommendations to the Secretary of Defense and other Department leaders on catalyzing innovation in the Department to strengthen our national security and future-proof our warfighting capabilities.

This study tackles internal barriers to innovation by identifying several key barriers, highlighting the expected outcomes once the barriers are resolved, and offers recommendations on how to resolve them. This study reflects the passion and commitment of the Defense Innovation Board members to drive change and scale innovation at the Department in support of our national defense mission and is supported by a rigorous research approach that triangulates academic insights, industry practice, and Department of Defense context and equities from all the Services practiced by the Defense Innovation Board research team.

Acknowledgements

Defense Innovation Board Members

Michael R. Bloomberg, Chair
Hon. Sue Gordon
Reid Hoffman
Admiral (Ret.) Mike Mullen
Charles Phillips
Hon. Mac Thornberry
with
Dr. Gilda Barabino
Mary Meeker
Hon. Dr. Will Roper
Ryan Swann

Defense Innovation Board Consultants

Wendy Anderson
Yisroel Brumer
Essye Miller
Chris Taylor

Executive Director

Dr. Marina Theodotou

Staff

Zackariah Crahen
Dr. Juan Merizalde

Khalia Alexander
Logan Hatfield
Melanie Heinlein
Christina Hilf
Abigail Linman
Jacob Sharpe
Elliot Silverberg

Executive Summary

To advise the Department of Defense on how to expedite innovation at scale, this Defense Innovation Board (DIB) study focused on removing internal barriers to innovation in the Department. The study identifies seven broad domains that reach across aspects of security, acquisition, information technology, and human capital. These seven domains encapsulate 13 different internal barriers hindering innovation, and present 17 specific, actionable recommendations to each barrier to facilitate, adopt, and scale innovation across the Department.

A key, overarching recommendation resulting from this study is the need for the Secretary of Defense to reinforce that all leaders are responsible and accountable for innovation across the Department. The status quo will persist unless there is a shift towards a culture of innovation and risk-taking, driven by empowered senior leadership. All leaders must transform processes and procedures under their command to make them faster, easier, more useful, and more inclusive of the entire ecosystem (both inside and outside government) to which they are responsible.

The study finds that the Defense Counterintelligence and Security Agency (DCSA) has the potential to become a force-multiplier. This would be achieved by granting the Director the necessary authorities to modernize personnel clearance management, collaborate with agencies that have overlapping responsibilities, and update outdated regulations to account for the current threat climate and the needs of the defense security enterprise. In order to support the rapidly changing innovation landscape, authorities to operate need to be reciprocal. However, the current practice of issuing requests for proposals hampers agility, creates a misalignment between needs and incentives, reduces the capacity of services and the Office of the Secretary of Defense (OSD) to support the warfighter, and increases risk to the Department of Defense. Moreover, the Department is not currently a preferred business partner and must standardize its bidding practices to align them with industry standards. This includes adopting industry established pitch practices, and maximizing the visibility of existing contracts to mitigate redundancies to curtail unnecessary administrative burdens, especially for vendors. In addition, the lack of centralized management in enterprise licensing prevents the creation of a competitive environment and hinders the delivery of the best value to the Department, agencies, and services. Finally, inadequate market research and under-utilization of innovation organizations for discovering existing technology that meets warfighter needs, leads to further redundancies, inefficient acquisition processes, and requires an expanded implementation of dual-use technology combined with cross-functional teams, earlier in the capability development cycle.

This study reflects months of research, however, it is neither exhaustive nor a panacea to the full scope of internal innovation barriers impeding the Department. Moreover, this study was developed through the insights and expertise of the DIB members and consultants, the triangulation of academic research, industry practices, and targeted Department engagements. It presents actions that can be taken immediately, warrant NDAA inclusion, and will scale innovation across the Department.

The Imperative of Lowering Barriers to Innovation

Defense Innovation – which we define as the ability to rapidly develop and integrate new systems and technology, and employ them at the speed and scale necessary to maximize warfighter mission capabilities – is vital to the U.S. military's strategic advantage as it confronts the pressing challenges of a complex, evolving geopolitical landscape in this decisive decade.

Over the past three years, the U.S. Department of Defense introduced several initiatives to invest in emerging capabilities. These efforts include:

- The 2021 Department of Defense AI and Data Acceleration initiative to rapidly advance data and AI-dependent concepts;
- The 2022 establishment of the Innovation Pathways website, allowing a gateway for small businesses to engage with the Pentagon on new systems;
- The 2022 launch of the Rapid Defense Experimentation Reserve, which offers edge experimentation to new equipment to move prototypes through validation to production;
- The 2022 establishment of Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO), the office responsible for accelerating Department of Defense's adoption of data, analytics, and AI to generate decision advantage across the Department, "from the boardroom to the warfighter;
- The 2023 Department of Defense Software Modernization Strategy and Implementation Plan;
- The 2023 National Defense Science and Technology Strategy;
- This year's establishment of the Pentagon's Office of Strategic Capital, which will soon employ financial tools such as loans and guarantees to support startup-built solutions; and
- The realignment, earlier this year, of the Defense Innovation Unit (DIU) to serve as a direct report to the Secretary of Defense.

However, despite these critical efforts, defense innovation remains hampered by the intricacy of our defense structure, arguably the world's most complex business enterprise. This tangled system, influenced significantly by external forces, stakeholder pressures, congressional oversight, federal regulations, and suboptimal procurement processes, hinders rapid adoption and ultimately, implementation of new systems.

We can no longer wait decades, or much less years, to scale innovation at the Department. Our ability to rapidly deliver capability at scale to the warfighter is critical to ensuring the United States military retains its advantage over competitors and adversaries alike. Our ability to ensure enduring technological superiority hinges on how fast we can remove the barriers internal to the Department that hamper innovation adoption.

This study is structured as follows: each of the seven domains constitute a section and each section provides specific barriers to innovation. For each domain, a desired broad outcome is listed, along with micro-level barriers, recommendations or sets of recommendations to overcome those barriers, and associated outcomes which influence the overall macro-level domain. For domains 3, 6, and 7, only the domain barrier, outcome, and recommendation are presented.

Barriers and Recommendations to Innovation

1. Domain: Leadership

The DIB examined Leadership across the Department for each domain and determined barriers to innovation will persist without senior leadership buy-in to instill urgency, and provide support to middle and junior leaders to take big risks and act as change agents on the frontlines.

Outcome: Senior leaders move at speed and scale.

Barrier: Breaking the status quo of engrained barriers to innovation necessitates an urgency to drive transformative change across the Department, championed by senior leadership, but that is presently absent at scale across the Department.

Recommendation: The DIB recommends within one year, SECDEF mandates metrics for each recommendation below will be developed and become the basis for personnel performance evaluation.

2. Domain: Security

The DIB examined Security across leadership, facilities and personnel management, and determined that neither the authorities exist to effectively manage facilities and personnel, nor are the policies in place for the agencies within whose purview it is to do so.

Outcome: The Department of Defense affords leadership the authority to collaborate across agencies to reduce cost, increase efficiency, expand access, and leverage facility and personnel security management as a Department asset to drive mission-capability development and ensure the security of the Department's people, systems, and property.

Authority

Barrier: The Defense Counterintelligence and Security Agency (DCSA) Director lacks the authority commensurate with their responsibility for managing Department-level relationships across personal, physical, and industrial security.

Recommendation: The DIB recommends that within one year, DCSA will complete a review of security needs and responsible entities, to include recommendations for how authorities must be realigned to allow efficient and effective progress against the needs of the Department and all supporting elements of the security ecosystem.

Secure Facilities

SCIF Access and Management

Barrier: The existing limitations for sensitive compartmented information facilities (SCIFs) access, exclusively available only to owners, obstruct other agencies, small businesses, and those seeking participation in defense-related R&D and contract competition. Additionally, SCIF ownership transfer necessitates costly and time-consuming rewiring or complete reconstruction, adding time, complexity and expense.

Recommendation: The DIB recommends that DCSA and parallel agencies establish a central credentialing authority to oversee SCIFs throughout the Department of Defense. This authority should enable external stakeholders and non-parent owners of SCIFs to access these facilities, provided they meet established clearance requirements. Through this approach, it would not only enhance security in reforming SCIFs as a Department of Defense asset, but also facilitate easier engagement with external entities, streamlining access and improving overall efficiency. By eliminating unnecessary complications, these measures will help break down fundamental barriers that hinder efficient collaboration and defense-related activities.

ICD 705 Standards

Barrier: The ICD 705 Standard[1] is a set of security requirements for SCIFs, which are specially designed buildings or rooms that house classified information and activities. However, the standard is outdated and neither accounts for the current capabilities of adversaries, who may use advanced technologies and methods to breach the security of the SCIFs, nor the needs of the defense innovation ecosystem. The standard also hinders the new construction and retrofitting of the facilities, as well as the acquisition and production of the equipment, by imposing rigid and costly specifications that may not be necessary or effective.

Recommendation: The DIB recommends that DCSA, the Defense Intelligence Agency (DIA) and National Security Agency (NSA) collaboratively develop and implement an updated security standard for SCIFs to overcome the outdated and inadequate ICD 705 Standards. The new standard should be based on four actions: (1) improving risk analysis support to the Authorizing Official (AO) and the Senior Security Manager (SSM) in identifying the adversarial capabilities that use advanced breaching technique, tactics, and procedures, and conducting comprehensive risk assessments of the existing and planned SCIFs accordingly; (2) developing a set of security measures that are tailored to the specific risks and needs of each SCIF, and that balance the security, cost, and performance objectives; (3) implementing a continuous monitoring and evaluation system that tracks the effectiveness and efficiency of the security measures, and that allows for timely adjustments and improvements; and (4) implementing direct collaboration and coordination between DCSA, the DIA and NSA, on the technical and physical aspects of SCIFs, and leveraging their expertise and resources to ensure the security and resilience of SCIFs as a Department-wide asset.

Personnel Vetting

Establish Enduring Clearance Reciprocity

Barrier: The expiration of security clearances after a fixed period upon exiting government positions creates a disincentive for individuals to re-enter government employment or pursue private sector roles that require clearances. This situation hinders the Department's ability to attract and retain highly skilled personnel.

Recommendation: The DIB recommends that DCSA provide clearance holders, including contractors and Special Government Employees(SGEs), the option to pay for Continuous Vetting of their clearances following their departure from active duty or related positions. DCSA offers Continuous Vetting for national security positions at a cost-effective rate. By enabling individuals to maintain their clearances, it promotes easier reentry into government employment and private sector positions that require clearances. Consequently, this proactive measure also helps reinforce security as a Department-wide asset, attracting and retaining skilled personnel more effectively, and reducing barriers that hinder efficient engagement with the Department.

Upgrade or Replace NBIS

Barrier: Reforms of the National Background Investigation Services (NBIS) system over the past five years have proven to be insufficient to meet the needs of DCSA[2].

Recommendation: The DIB recommends that DCSA allocate funding or other resources to fill any gaps that exist which have thus far impeded NBIS from meeting its mission capability requirements. If NBIS is determined to be insufficient, obsolete, or cost / time prohibitive, fund NBIS as much as is needed to continue DCSA operations, with any additional or future funding to be allocated, including

[1] ICS 705 Standard
https://www.dni.gov/files/NCSC/documents/Regulations/ICS-705-1.pdf

[2] For more information on personnel vetting see GAO's report
https://www.gao.gov/products/gao-22-104093

associated cost and schedule, to research and development on an altogether new system.

3. Domain: A Continuous Authority to Operate (ATO) Software Strategy

The DIB examined the number and variety of cloud landing zones in place across the Department. Examples of operational landing zones that increase scale are ADCP, Party Bus, Game Warden, Black Pearl, ARCUS, and ODIN but are not enough. Too little access to cloud landing zones creates a bottleneck for technologies the Department needs in place, consequently driving up cost through delayed processes.

Outcome: A faster, more secure deployment of SaaS products across different cloud environments and impact levels, through the implementation of reciprocity and embracing a Continuous Authority to Operate model that increases the number and variety of cloud landing zones available for its technologies, reducing the cost and time of authorization processes.

Recommendation: The DIB recommends the CIO employs a policy of direct reciprocity for any SaaS product with an ATO in an approved cloud environment, facilitating collaboration with other Department users within the same cloud environment at the same impact level. In addition, the Department embraces a "Continuous Authority to Operate" strategy to ensure rapid software updates without the requirement for new ATOs. This approach will enhance efficiency and eliminates the need for authorizing officials to force companies through repetitive ATO processes.

4. Domain: Contracting Processes

The DIB examined how the Department conducts its contracting activities and determined RFPs are too cumbersome, filled with unnecessary and overly restrictive information, oriented on a specifications-based model for selection, and associated SOWs that often create self-imposed risk to the Department. Contractors and non-traditional businesses alike struggle with these complexities and may cause them not to bid for a technology that the Department absolutely needs.

Outcome: Awarded contracts are mission-oriented, outcomes-driven, drive competition and innovation opportunities, maximize utility of the product or system to the end-user, and mitigate risk to the Department.

RFP Length Restrictions

Recommendation: The DIB recommends the Office of the Under Secretary for Acquisition and Sustainment (OSD A&S) require exceptions to policy for any RFPs to exceed three pages in order to streamline the acquisition process and attract more innovative and non-traditional contractors. RFPs need only to clearly state the desired outcomes, mission capability, and features of the solution–rather than impose extensive and rigid specifications that may limit the creativity and flexibility of the contractors.

Demonstration Requirements

Recommendation: The DIB recommends OSD A&S require RFPs to include criteria for contractor demonstrations that will provide evidence of their capabilities and expertise, either by demonstrating a prototype or by interviewing the technologists who would build the solution. As a result, the Department can evaluate the potential of the contractors based on their actual performance and suitability, rather than on their compliance with bureaucratic requirements. In addition, it affords Program Executive Offices (PEOs) the opportunity to fully understand a proposed solution to ensure it does in fact meet a mission capability need.

Data and Intellectual Property Sharing

Recommendation: The DIB recommends that when contracts are awarded, SOWs must make clear, mission-critical, data sharing authorizations with IP owners as a component of any contract award to ensure the Department is not beholden to single-solution

sustainment providers that inhibit warfighting capacity or mission readiness.

Contract Structure

Recommendation: The DIB recommends OSD A&S transition from time-material contracts that hinder agility, add to cost, and incur more risk to the Department, to expanded use of contracting alternatives, such as firm-fixed price, which establish measurable and enforceable expectations.

5. Domain: Aligning Government and Industry Processes

The DIB examined the effectiveness of the Department's industry pathways and determined it lacks satisfactory processes to allow private sector vendors to consider the Department as an attractive business partner.

Outcome: Industry aligned, Department of Defense-wide, proposal processes proliferate access to and increase the appeal of the Department as a business partner, founded upon pools of trusted vendors, maximizing SBIR phase visibility, and in support of thorough market research that reduces duplication of effort and flattens the acquisition and sustainment cycle.

Department of Defense-Specific Requirements

Barrier: Companies, especially first-time applicants, face formidable barriers when seeking to do business with the Department due to a unique-to-Department of Defense process that imposes significant administrative cost.

Recommendation: To lower the entry barrier for non-traditional businesses, the DIB recommends OSD A&S align its contracting processes with private sector practices. This includes introducing a standardized, Department-wide proposal format that resembles commercial practices, such as pitch decks, and adopting pricing models similar to commercial "proof-of-concept" contracts. The proposal format should be easy to prepare and submit, and the Department should commit to rapid award timelines.

SBIR Visibility

Barrier: The Department does not have a convenient, enterprise-wide, database solution for the services and Department of Defense Field Activities (DAFAs) to see the funding lineage of awarded SBIRs (both funded and unfunded) from Phase 1 to Phase 2, or at all from Phase 2 to 3, with the fidelity required to be useful in acquisition processes.

Recommendation: The DIB recommends OSD A&S improves existing platforms or establishes a one-stop, Department of Defense-wide and managed SBIR platform, replete with relevant information such as vendor, contract type, period of performance, value, performance ratings, contracting officer, Contracting Officer's Technical Representative (COTR), Department customer complete POC information, and the associated funding lineage whether selected with or without funding through each phase, and that can be imported into Advana as an additional avenue to maximize utility.

Contract Development

Barrier: Emphasis is not placed on conducting thorough enough market research of existing technologies or best practices that meet a specific mission capability need.

Recommendation: The DIB recommends OSD A&S require PEOs to justify awarding contracts with detailed market research at the beginning of the capability development cycle, in conjunction with cross-functional teams (CFTs), that demonstrates a need not presently satisfied by an existing system or service.

Business Vetting

Barrier: The Department imposes excessive security requirements on non-traditional businesses, limiting their ability to showcase their capabilities and consequently, unnecessarily reduces the pool of potential candidates.

Recommendation: To increase the diversity and quality of potential candidates, the DIB recommends OSD A&S avoid imposing security requirements on non-traditional businesses in RFPs until the government has a clear understanding of their capabilities. The Department should also create an independent classification system for potential bidders, which would allow them to demonstrate their suitability for different types of contracts without revealing sensitive information.

6. Domain: Enterprise License Agreements (ELAs)

The DIB examined the Department's Enterprise License Agreements strategy and determined vendors undermine this strategy by offering better pricing to larger organizations, adjusting capabilities with unique packages, resulting in routinely approved waivers that add to administrative costs and ultimately erode value.

Outcome: Enterprise software is purchased through a single entity, seamlessly integrating Department agencies and services, enabling data transferability, promoting competition, and streamlining procurement of the latest mission-critical or back-office software.

Recommendation: The DIB recommends the Chief Information Officer (CIO) enforce Secretary or Deputy Secretary-level direction across the defense software enterprise, establishing a Department-level program office to collaboratively define user requirements, manage acquisitions and contract modifications, establish robust business rules for compliance, communicate the Department's strategic vision, implement a limited waiver process under DSD authority, restrict vendors from approaching multiple organizations, and centralize IT resources at the Department level (e.g., Department of Defense CIO, Navy, DISA) for streamlined execution.

7. Domain: Dual-Use Technologies

The DIB examined the Department's ability to acquire dual-use technologies and determined it encounters significant self-imposed obstacles in adopting commercial dual-use technology. Such obstacles include locking in specific vendors, limiting investment in start-up research and development, limited market agility, and supply chain challenges. Specifically, the current burdensome acquisition process around dual-use technologies forces non-traditional start-up companies through a painful, long, and costly journey in their effort to traverse the valley of death[3]. Currently, the Department requires companies to first create a viable product for commercial use, and then, if the product is still viable commercially, to approach the Department and adapt the product for use in defense. For instance, a start-up that develops AI for swarm drones could ultimately contract with the Department, but not before spending copious amounts of resources and time to succeed in the commercial space first. This adds risk to the Department by allowing market forces to be the gatekeeper of potentially mission-critical systems, rather than the Department making this determination on the front end to ensure such a system is not overlooked. Another self-imposed constraint is the concentration of the defense industrial base to a handful of large primes who are consistently contracted to tackle large scale defense challenges. This setup does not allow room for smaller start-ups, who may be successful in their dual-use technology efforts, and forces them to simply sub-contract for the primes, which in turn drives vendor lock, limited market agility, and creates supply chain challenges.

Outcome: The Department looks first for an existing commercial solution, and becomes a better customer by providing earlier, clearer,

[3] For more information on the valley of death see https://warontherocks.com/2022/09/reliance-on-dual-use-technology-is-a-trap/

faster, and more frequent feedback to start-ups and vendors, and adopts a flexible and agile approach to acquiring and using commercial dual-use technology.

Recommendations: First, to overcome the barrier of commercial dual-use technology the DIB recommends that the OSD A&S its communication and engagement with the commercial sector and the entrepreneurial community including venture capitalists and founders by leveraging its existing networks and platforms, such as the Defense Innovation Unit, the Defense Advanced Research Projects Agency, and the Small Business Innovation Research program. This would help to build trust and understanding, to exchange information and feedback, and to find common interests and goals that can lead to collaboration and cooperation. Second, the Department should adopt industry best practices in developing a flexible and agile approach to acquiring and using commercial dual-use technology by connecting the acquisition process to the research and development funnel earlier to alleviate the pressure from start-ups involved in dual-use development to first 'make it' in the commercial sector. Third, the Department should scale its efforts on its people innovation readiness[4], which in turn can foster and cultivate a culture of innovation by empowering personnel to develop innovator behaviors such as curiosity, growth mindset, and risk-taking that facilitate the discovery, consideration, and adoption of dual-use technologies to optimize the warfighter capabilities.

[4] For more information on people innovation readiness see www.dau.edu/Innovatetowin

Conclusion

Scaling innovation at the Department of Defense is a major challenge and one that the Department has been attempting to tackle for many years. Today, with Department-wide initiatives such as Replicator under way, scaling innovation is becoming easier. However, internal barriers still exist within the Department across several domains that until deliberately addressed, will continue to hinder many initiatives from scaling– including Replicator. The removal of such barriers can untether innovation from procedural, bureaucratic, and administrative encumbrances, and facilitate the delivery of warfighting capabilities at speed and scale.

This Defense Innovation Board study examined and distilled seven key innovation barrier domains, clearly illuminated the barrier, highlighted the expected outcome if the barrier is removed, and provided actionable and practical recommendations to tackle each domain and its barriers.

While these seven domains reach across many aspects of the defense innovation ecosystem, they have not been confronted with the specificity and clarity necessary to facilitate their resolution and removal. To do so, this study concludes leaders across all Department of Defense components must be both empowered and held accountable to drive change, be proactive, innovative, and execute with the urgency deserving of the moment and in support of the warfighter.