SHINING A LIGHT ON THE DEFENSE DEPARTMENT'S INDUSTRIAL BASE PROBLEMS

Jeff Decker and Noah Sheinbaum

With the recent release of the National Defense Industrial Strategy, the Defense Department has acknowledged the urgency of strengthening the linkages between a healthy defense industrial base and U.S. military power. Despite this, the views of defense-tech companies are often overlooked. Using original data derived from a new survey, Jeff Decker and Noah Sheinbaum offer a number of steps the Defense Department can take to lower the barriers that companies face in converting disruptive commercial technologies into widescale defense capabilities.

From bands to chiefdoms to states, political structures historically evolved to provide more resources (e.g., land, labor, and capital goods), which led to more effective militaries and, subsequently, better security and prospects for survival.[1] These efficiencies of scale, both in terms of manpower and resources, established an irreducible relationship between a state's industrial base, military power, and security. A state incapable of leveraging industry for its own defense may struggle to project power and establish security.

In 2014, the Defense Department began to acknowledge that declining government-led research and development activity meant it needed to seek access to defense-relevant technologies developed and brought to market by commercial partners. Over the past decade, the department increased its ability to partner with commercial companies by establishing new organizations (e.g., Defense Innovation Unit, AFWERX, Army Applications Lab, and NavalX) and programs (e.g., Rapid Defense Experimentation Reserve, Accelerate the Procurement and Fielding of Innovative Technologies) to help defense personnel access the technologies they need. These new organizations and programs resulted in significant progress in attracting commercial companies and funding to the defense market. It is now easier than ever for companies to work with the Defense Department and raise capital while doing so. Yet, significant challenges remain.

On Jan. 11, the Defense Department released its first *National Defense Industrial Strategy*, laying out four strategic priorities to modernize and expand the U.S. defense industrial ecosystem.[2] The strategy is an acknowledgement that despite numerous acquisition improvements and record levels of private investment into the defense tech industry, companies struggle to move from the government's pilot stage to widespread adoption, the process known as crossing the "valley of death."[3] The valley of death causes thousands of companies to leave the defense market annually and has resulted in a 43 percent decline in small businesses in the defense industrial base over the last decade.[4] Overcoming the valley of death has been a primary concern of policymakers and defense personnel to ensure warfighters have access to rapid technological advancements that can change the conduct of warfare.[5]

The *National Defense Industrial Strategy* highlights a variety of issues in the industrial base and the Defense Department's inability to sufficiently leverage all aspects of it. Two of the four *National Defense Industrial Strategy* pillars — resilient supply chains and flexible acquisition — are directly tied to the U.S. government's desire to woo commercial companies to bring their capabilities to the defense market.[6] Yet, industrial strategy does not exist in a vacuum. The *National Defense Industrial Strategy* comes on the heels of the release of the Defense

[1] Jared Diamond, *Guns, Germs, and Steel: The Fates of Human Societies* (New York: Norton, 2005), 154.

[2] U.S. Department of Defense, *National Defense Industrial Strategy*, 2023, accessed January 11, 2024, https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf.

[3] Defense Innovation Board, *Terraforming the Valley of Death: Making the Defense Market Navigable for Startups*, 2023, accessed January 8, 2024, https://innovation.defense.gov/Portals/63/DIB_Terraforming%20the%20Valley%20of%20Death_230717_1.pdf.

[4] U.S. Government Accountability Office, *Small Business Contracting: Actions Needed to Implement and Monitor DOD's Small Business Strategy*, accessed January 8, 2024, https://www.gao.gov/products/gao-22-104621.

[5] U.S. Department of Defense, Summary of the 2018 *National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge*, accessed January 8, 2024, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[6] U.S. Department of Defense, *2022 National Defense Strategy of The United States of America*, accessed January 8, 2024, https://apps.dtic.mil/sti/trecms/pdf/AD1183514.pdf.

Department's 2023 *Small Business Strategy*[7] and the establishment of the Defense Innovation Board's task force focused on "Terraforming the Valley of Death."[8] These initiatives view the issue primarily from the government's perspective and lack sufficient quantitative data from the perspectives of companies that can illuminate the scale of the challenges they face in entering and growing in the federal market. We aim to fill that gap here, using survey data as well as our backgrounds in the defense industry, management consulting, university-based research, and military service.

Without rapid progress to improve the transition of novel commercial capabilities to widescale defense capabilities, the United States faces the bleak prospect of competing against an adversary with a superior modernized military. Neglecting the needs of the defense industrial base may cause companies to lose interest and instead choose to pursue commercial opportunities elsewhere. It may also cause investors to lose patience, resulting in fewer founders entering the national security space. This would result in the Defense Department facing a technology shortfall when it can least afford to do so.

About the Survey, Respondents, and Report

We collected data from a 10-question survey fielded in October and November 2023.[9] The questions focused on the issues companies face when partnering with the U.S. government. The survey was distributed to a network of Small Business Innovation Research (SBIR) and Small Business Technology Transition (STTR) grant recipients, consortiums supporting Other Transaction Authority opportunities, venture capital portfolios, personal networks, and public requests via LinkedIn and emails to companies previously or currently doing business with the U.S. government or seeking to do so.[10] It received 859 responses.

Respondents included a mix of companies from the defense industrial base as well as commercial businesses, ranging from small businesses to large corporations. Together, they represent a broad range of products, levels of experience in working with the government, and funding types.[11] [12]

Company Output	% of Respondents
Hardware	34%
Software	32%
Services	34%

Table 1. Which of these do you sell?

Government Experience	% of Respondents
None	23%
1-5 years	18%
6-10 years	15%
11-15 years	8%
15 or more years	34%
Unknown	2%

Table 2. How much experience has your founding team had working with or in government prior to founding?

Revenue Type	% of Respondents
Commercial	68%
Federal Research and Development	87%
Federal Operations and Maintenance or Procurement	29%
Non-Federal Government (State or Local)	33%
International Government	16%
Academic Grants	21%
Other	7%

Table 3. Please select all of the types of revenue that you have earned.

Investment Type	% of Respondents
Personal Capital	78%
Equity Investments from Friends and Family	33%
Private Venture Capital	24%
Corporate Venture Capital	11%
Debt	33%
Non-Dillutive Funding	82%

Table 4. Which of these have you used to fund your business?
Note: The composition of companies receiving private investment in this sample reflects the wider defense industrial base consisting of approximately 100,000 companies.

Findings

Our survey and research yielded five key findings on the most pressing needs and significant challenges companies face when working with the Defense Department. First, partnering with different types of companies requires different tactics. The U.S. government should develop unique approaches for partnering with each type of company. Receiving contract awards quickly is crucial for smaller companies and startups, whereas size is more important for companies with substantial commercial revenue. Second, Defense Department partnerships with new entrants to the federal market often falter because companies and buyers are disconnected. Companies struggle to identify customers and to align the users, buyers, and contracting officers who each play a role in a successful sale. Third, new entrants are unprepared to meet federal government requirements like technical certifications (e.g., airworthiness) or licensing requirements (e.g., authority to operate), which can impede technology transition and cause delays in award. Fourth, the U.S. government's overly assertive stance on intellectual property rights delays awards and shrinks the pool of companies willing to sell to the Defense Department. Finally, the difficulty companies face in obtaining security clearances and accessing physical and virtual classified environments limits the U.S. government's exposure to new or commercial capabilities. We expound on each of these findings in the following sections.

Policymakers and defense personnel will benefit from this work as it offers empirically based insights on the needs of companies as well as recommendations for how to improve the U.S. government's ability to adopt commercial technologies. Both insights and recommendations are essential to informing U.S. defense and industrial policy. Each individual recommendation would be a step forward, even if the entire package is not adopted.

Different Companies, Different Tactics

> *"As a small business, the cost of doing business with the federal government is steep, risky, and always uncertain." -Survey Respondent*

What companies need from the federal government depends on their size and previous record of success.

Companies dealing exclusively with the federal market are most focused on receiving contracts faster. Reducing the time that the government takes to award a contract is the top choice of 44 percent of respondents with operations and maintenance or procurement contracts, and 42 percent of respondents with more than 15 years of government experience.

On the other hand, companies with commercial revenue prefer larger contracts: 67 percent of companies with commercial revenue rate contract size first or second.

Companies offer a variety of perspectives on contract challenges in their commentary on this point. Some companies struggle to understand how the government buys products, while the government struggles to understand what companies need from a government partnership. One respondent mused: "It is becoming a joke out in industry about how little acquisition personnel, program managers, [and] 'innovation' personnel understand emerging technology rapid acquisition and adoption, especially from small business."

Several respondents were concerned about the long time it takes for the government to award a contract, even after a decision is made. These delays

[7] U.S. Department of Defense, *Small Business Strategy*, January 2023, accessed January 8, 2024, https://media.defense.gov/2023/Jan/26/2003150429/-1/-1/0/SMALL-BUSINESS-STRATEGY.PDF.

[8] Defense Innovation Board, *Terraforming the Valley of Death*.

[9] "Doing Business with the U.S. Government," Frontdoor Defense, accessed January 17, 2024, https://www.frontdoordefense.com/report.

[10] Other Transaction Authority refers to the authority of the Defense Department to carry out certain prototypes, research, and production projects. It was created to provide the necessary flexibility to adopt and incorporate business practices that reflect industry standards. "Contracts and Legal: Other Transaction Authority," AcqNotes: The Defense Acquisition Encyclopedia, accessed January 17, 2024, https://acqnotes.com/acqnote/careerfields/other-transaction-authority-ota.

[11] Non-dilutive funding is a type of capital financing that does not require a startup to surrender equity in exchange for funding. "Dilutive funding vs non-dilutive funding," Liquidity Group, accessed January 17, 2024, https://www.liquiditygroup.com/resource-funding/dilutive-funding-vs-non-dilutive-funding#:~:text=Non%2DDilutive%20Funding%20is%20any,%2C%20vouchers%2C%20and%20tax%20credits.

[12] "What is the Defense Industrial Base?," Institute for Defense and Business, accessed January 19, 2024, https://www.idb.org/what-is-the-defense-industrial-base/#:~:text=There%20are%20more%20than%20100,and%20services%20to%20the%20government.

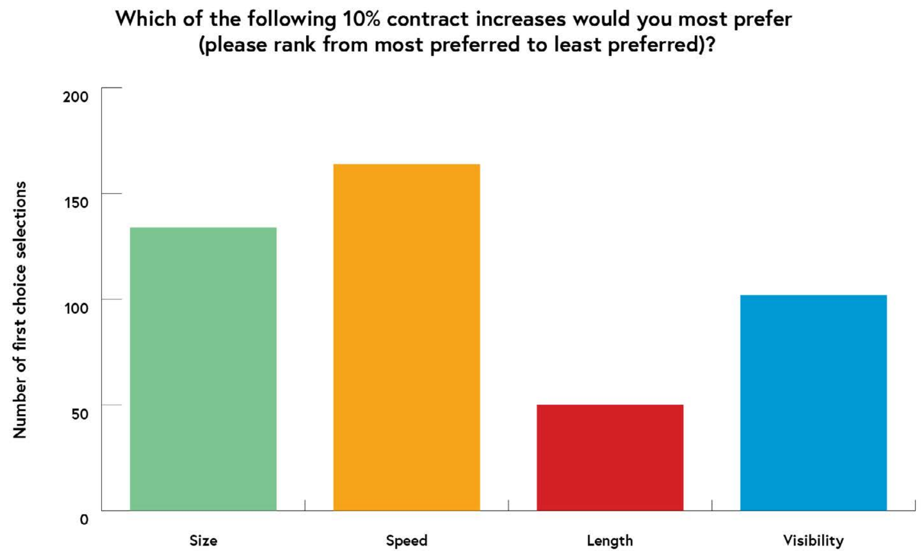

Figure 1. Contracts

can have acute financial impacts on small businesses. One respondent noted: "As a small business we can't afford to float labor costs and wait around for the government to finalize a contract. They are destroying their own productivity with bureaucracy and delays." Another claimed that the "[long] time to award for research and development grants almost nullifies its utility." Yet another called out slow time-to-award, which makes "it very difficult to project a runway with a nine month turn-around."

The results suggest the federal government should recognize and appreciate variations in company type when developing and carrying out an acquisition strategy.

If the Defense Department is serious about the goal of "diversifying its supplier base and investing in new production methods," as stated in the *National Defense Industrial Strategy*,[13] and implementing its "fast follower" strategy, it should offer larger, more secure revenue for firms with existing commercial products.[14] Companies require financial upside from the defense market to justify resource investments in defense sales and product customizations. This means that "picking some winners"[15] — awarding fewer contracts for larger sums of money and rapidly scaling successful pilot projects to production — is not just a smart transition strategy, but an essential market signal to startups and investors that the federal market holds sufficient promise.[16] Larger contracts will create longer runways to deal with Defense Department timelines, which will help fast-follower companies devote resources to pursuing government opportunities.

On the other hand, securing a contract in a timely manner is even more important to newer companies relying on the government as a primary revenue source. Some survey respondents indicated that contracting delays created problems such as prohibitive costs in keeping experts on the payroll while the company waited for a contract to be awarded. In addition, long award times make it more difficult for companies to successfully execute their contracts, as government sponsors often transition to new roles before contracts are awarded. This leaves companies without internal support for initiatives when they are finally under contract. If the U.S. government wants to continue attracting new companies to the defense market, it should award contracts quicker.

What should the Defense Department do to address this problem? One option would be to publish an annual transition playbook detailing examples of successful company transition pathways to serve as guides for similar companies and program offices to follow. The Defense Department can help companies replicate technology transitions from introducing their technology as a test, or pilot, all the way to full-scale production manufacturing at scale. In addition to explaining the planning, programming, budgeting, and execution process, the playbook should include a set of transition spotlight case studies, detailing the steps successful companies took to transition. Entities such as AFWERX, DIU, NavalX, and others would submit exemplary case studies of companies each year. The playbook would be organized by technology area (e.g., autonomy, quantum, and energy), service, and other key delimiters to help companies and program offices identify similarities. Companies could then create a defined deployment pathway based on these case studies, tailored to their technical focus, needs, and maturity.

Additionally, the government could clarify the acquisition process to attract the right companies for the desired capability — and help companies determine when not to bid. Expanding and increasing the capacity of the defense industrial base means not only attracting more companies to the market but also helping them determine which awards to pursue.[17] Program managers and contracting officers can work with companies to develop acquisition strategies that expand the vendor pool while also helping companies filter through relevant opportunities. Government acquisition offices should be required to release their determination of contracting approach in their market research or initial solicitation, including information about the competitive process, timeline, contract type, and evaluation criteria. Each office responsible for an acquisition should publish an estimated time to award the contract, and then assess annual accuracy, so that vendors can evaluate the potential costs and benefits of a response and the timeliness of the office. Furthermore, acquisition officials should be seen as strategic advisors to the program office, communicating the commander's intent to craft a strategy that delivers capability and provides a path to scale up rapidly if successful or terminate quickly if unsuccessful. While not every contract will be built for speed, the Defense Department can provide more information to help companies self-select where their time will be well-spent.

Expanding and increasing the capacity of the defense industrial base means not only attracting more companies to the market but also helping them determine which awards to pursue.

Disconnected From the Buyers

"If you don't start with shot-callers, you're going nowhere fast." -Survey Respondent

Companies need connectivity to government program offices because they control budgets.

Among all respondents, 43 percent ranked a program officer the government representative they most prefer to meet, while end-users were the clear second choice. Meanwhile, 27 percent of respondents ranked end-users the most important.

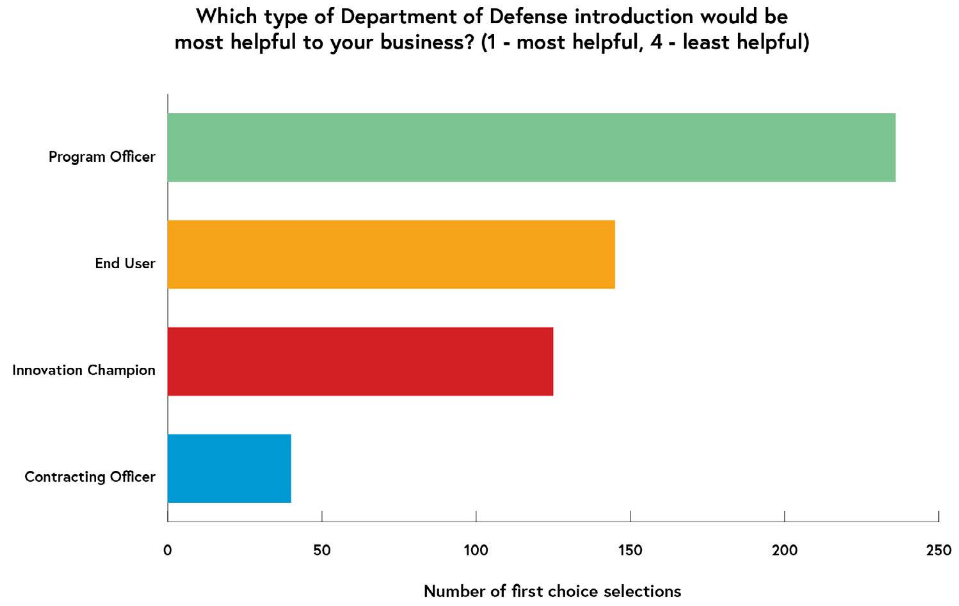

Figure 2. Introductions

[13] U.S. Department of Defense, *National Defense Industrial Strategy*, 19.

[14] David Vergun, "DOD Modernization Relies on Rapidly Leveraging Commercial Technology," *DOD News*, January 25, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3277453/dod-modernization-relies-on-rapidly-leveraging-commercial-technology/.

[15] Stew Magnuson, "SPECIAL REPORT: Pentagon Makes Moves to Speed Up Tech Transition," *National Defense*, February 14, 2023, https://www.nationaldefensemagazine.org/articles/2023/2/14/pentagon-makes-moves-to-speed-up-tech-transition.

[16] Lara Seligman, "Pentagon Criticized for 'Spray and Pray' Approach to Innovation," *Foreign Policy*, October 16, 2018, https://foreignpolicy.com/2018/10/16/why-the-pentagons-spray-and-pray-approach-isnt-working-investment-technology-china/.

[17] Tony Bertuca, "DOD pushing new defense industrial strategy to expand weapons stockpiles," *Inside Defense*, October 25, 2023, https://insidedefense.com/share/219411.

The preference for program officer introductions cuts across all types and sizes of companies, regardless of founder experience, product type (i.e., software, hardware, or services), funding raised, and revenue earned.

Survey respondents did not see much value in connecting with contracting officers. However, of the 7 percent of respondents who ranked contracting officers as their most preferred government contact, nearly half had earned or are actively pursuing operations and maintenance or procurement contracts.

Most respondents believe that program offices are the gateway for successfully transitioning their pilot awards into production contracts. One respondent explained that "businesses hope for transition into longer-term relationships with the government; not just quick research and development efforts that get nowhere" and while "users are very important to delivering the right/best solution...if [program executive offices] aren't on board, it's a short-lived opportunity." Another respondent put it more bluntly: "If there is no budget, you [the company] have zero chance of success."

Overall, respondents viewed program offices as critical to scaling early pilot contracts, through programs like SBIR/STTR, to production. One small business entrepreneur stated: "It can be very challenging to mature a program from SBIR-level funding to direct program office. The challenges are largely non-technical (e.g., arranging a meeting to get all the key decision-makers in a room at the same time, competing with lower-quality versions of similar capabilities that have been developed by government labs)." They went even further to suggest that "having a clear vision and aligning with key stakeholders from the outset of what success looks like would go a long way to de-conflicting overlap with existing government-led initiatives."

Numerous respondents also provided their perception of contracting officers. Many were dismissive, with one respondent writing that "contracting officers don't actually make any favorable decisions, they just implement." Another wrote that "contracting officers simply manage the contracts but lack the whole picture to move the project forward." However, some expressed appreciation for these officials. One respondent exclaimed: "If you find a good contracting officer, you never let them go!"

It is not surprising that companies want to connect with program offices that control budgets. Nevertheless, these results are notable in that they suggest that the Defense Department has made significant progress in the past eight years on another front. The department took on the challenge of connecting companies to end-users by establishing entities such as the Army Applications Lab and the U.S. Cyber Command's Tech Outreach Division to improve entrepreneurs' understanding of which problems their solutions address and who might benefit from their solution. Moreover, entities such as the Air Force Spark Cells, Defense Ventures Fellows, and Defense Entrepreneurs Forum, among others, have increased the interest and willingness of servicemembers to engage directly with industry, and Phase I SBIRs provided the contractual basis for enhanced engagement between companies and government.[18]

Companies report that having end-user support, while necessary, is insufficient to win production contracts with the government. Even seasoned entrepreneurs with government experience struggle to navigate the Defense Department's acquisition bureaucracy, to turn end-user enthusiasm into programmatic requirements and meaningful business. The failure to connect companies and programmatic buyers is inhibiting companies from transitioning technologies to the warfighter. Pursuing commercialization objectives (Phase III) is not a guaranteed next step in the SBIR program. Rather, it refers to the sole-source authority companies can use if they successfully complete any previous phase of SBIR work. Companies can technically enter Phase III when a government customer obligates funds and issues their own contract. However, there is no guarantee that performing on a pilot contract will yield programmatic interest, funding, or pathways to continuing business. Companies need access to program offices.

Most companies view contracting officers solely as implementers or barriers to overcome, as paper-pushers as opposed to key influencers in the acquisitions process. "Contracting officers typically are the roadblock," as one respondent put it, typifies this sentiment. But this may be to their own detriment. Companies that have successfully earned defense revenue recognize that contracting officers are critical to success, especially in accelerating the speed with which a contract is awarded. Put simply, contracting officers are an underappreciated key to successful transitions. Few commercial companies fully understand the government acquisition process. Contracting officers can translate strategic guidance into action — making decisions about which type of contract to use, how long it takes, what intellectual property rights a company receives — and can set a company up for repeat business or, alternatively, leave them struggling to re-engage. Companies will need to shift their thinking about contracting officers if they are to be successful.

[18] The SBIR program consists of three phases: Phase I establishes the feasibility and commercial potential of a technology, Phase II continues the research and development efforts of Phase I, and Phase III pursues commercialization goals. "America's Seed Fund: Powered by the Small Business Administration," U.S. Small Business Administration, accessed January 19, 2024, https://beta.www.sbir.gov.

Companies that have successfully earned defense revenue recognize that contracting officers are critical to success, especially in accelerating the speed with which a contract is awarded.

How can the government do a better job of connecting companies to buyers? First, the Defense Department could create more meaningful opportunities for companies to collaborate with program offices before a contract is awarded. Making it easier for companies to identify and engage relevant program officers would enhance the government's ability to take advantage of commercial technologies. Industry days are often one-sided conversations in which companies learn about abstract government requirements rather than two-way learning opportunities to shape future requirements based on end-user needs and technological capabilities. Acquisition organizations such as the Defense Innovation Unit and AFWERX can bring together relevant program offices, end-users, contracting officers, and industry partners to inform new requirements, increase companies' awareness of technical readiness, and apprise the government of the benefits non-traditional companies are able to offer.

Companies engaging in such opportunities for collaboration could gain a better appreciation for the acquisition process and the vital role contracting officers play within it. The Army's Soldier Center, for example, has succeeded in helping defense organizations understand the latest commercial technology, while connecting companies to program offices and contracting officers.[19] In addition, dialogue between government personnel and entrepreneurs can shape an acquisition strategy to ensure it meets both government and commercial needs before issuing a request for proposal. The recently established Mission Acceleration Center network could provide great spaces for these engagements. Alternatively, these engagements could be included within "technology insertions" activities, which some program offices, like submarines, hold approximately every other year to integrate new technology into existing products.[20] Crucially, these engagements should educate companies about the best opportunities to engage program officers, and who to engage and with what material, to maximize chances of success and minimize wasted time.

Additionally, Defense Department pilot sponsors should identify, engage, and share information with relevant program offices from the start of pilot contracts. Companies and end-users know that the goal is a successful transition from pilot to production through a program office. Successfully making the jump requires companies and end-user organizations to mitigate perception of risk and engage with the program office well in advance. Pilot sponsors can identify key performance indicators for the existing programmatic capability a pilot seeks to replace and share pilot performance information with relevant program offices early on. While many pilots are too small to be of interest to major programs, early communication would help to build familiarity and trust, allowing the programs to monitor the maturity of a capability. This would serve the dual purpose of increasing visibility into new technologies for the program office while giving successful pilots a greater chance of transitioning inside the Defense Department.

Unprepared for Technical Transition

> *"Certifications and compliance requirements [are] highly complicated to navigate." - Survey Respondent*

Currently, most companies are not prepared to meet the compliance requirements necessary for federal government production contracts. The Defense Department requires technologies to be tested and evaluated, assessed for risk, and approved for use in a variety of operational environments.

Most respondents do not have any government license or certification, such as an Authority to Operate: 43 percent of respondents reported receiving some government license or certification, while 47 percent have not. Notably, of those that have received a license or certification, nearly half have an operations and maintenance or procurement contract. This reinforces the point that companies that do transition from pilot to production will often require certification.

The Authority to Operate is the most common certification, held by nearly one-third of those certified. Among software companies, 49 percent have an Authority to Operate, as do 56 percent of companies with operations and maintenance or procurement contracts.

[19] Jane Benson, "Soldier Center hosts U.S. Army Small Unmanned Aircraft System Technology Innovation Network Event," *DEVCOM Soldier Center Public Affairs*, November 3, 2020, https://www.army.mil/article/240535/soldier_center_hosts_u_s_army_small_unmanned_aircraft_system_technology_innovation_network_event.

[20] Clive Kerr, Robert Phaal, and David Probert, "Technology insertion in the defence industry: A primer," *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture* (August 2008), https://doi.org/10.1243/09544054JEM1080.

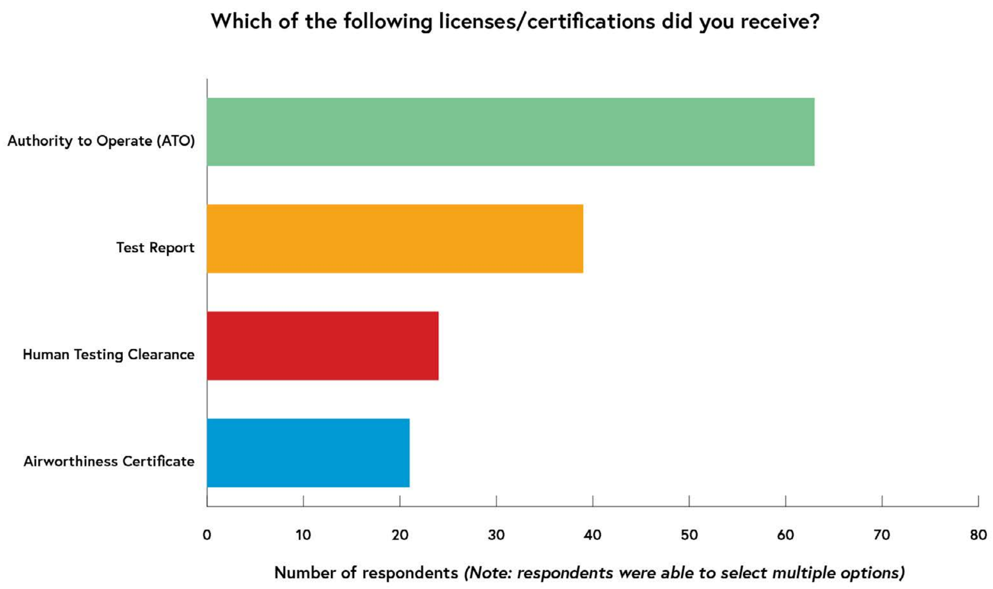

Figure 3. Licenses and Certifications

The problems companies have with compliance relate to being unaware that compliance requirements exist, as well as difficulty in completing the steps needed to obtain certifications and licenses. Companies are willing to comply but are often unaware of what certifications or licenses are required. Government customers are often unwilling to contract with companies that are not already certified. Knowledge of these requirements is an essential prerequisite to successfully navigating them. "The biggest challenge is gaining familiarity with processes. Processes are generally good but require experience to navigate," one respondent explained. "The process of going through this type of certification needs to be streamlined and easier, but it is important," another respondent shared. Another respondent reported that the government even canceled the award after learning that the company lacked a particular certification during contracting.

Multiple respondents noted that certifications are too expensive and do not account for the limitations of small businesses and newer companies: "The certifications required are not conducive to small business. The business can go out of business while trying to obtain them." The *National Defense Industrial Strategy* acknowledges this risk as well, recommending that the government "mitigate cybersecurity costs of entry to work in the defense industrial ecosystem."[21] But challenges go beyond cybersecurity compliance. Respondents highlighted the cost of certifications when a government customer is unwilling or unable to pay for it. "The certification process and requirements price out smaller companies," one respondent explained. Companies that try to navigate government certification processes often report difficulty in obtaining them. One respondent was concerned that "government application of security requirements … place a barrier to continuing work with no commensurate offer of assistance in obtaining the appropriate infrastructure."

The disconnect occurs because few pilot contracts require companies to obtain government licenses or certifications, but virtually all production contracts demand them.

Companies need a better understanding of the array of licenses and certifications they need to deploy their capabilities, and on what timeline, so they can build, budget, and plan appropriately to avoid costly delays and disruptions. Small or new companies do not have the large compliance departments to handle the administration of these requirements, nor the budgets to pay for some of these requirements out-of-pocket. They therefore need sufficient warning to ensure they are budgeted for any contract, no matter the cost (e.g., airworthiness certifications can cost upwards of $2 million).

Even in cases when a company has a total understanding of the required compliance activities, they still face additional hurdles. One issue is the chicken-and-egg problem: Companies need to have a contract to be eligible for most licenses and certifications, but they must have those licenses and certifications to receive a production contract in the first place. Another hurdle is that most innovative commercial technology acquisitions tend to be smaller in size and are therefore deprioritized for testing in government facilities. The result is that the smallest awards can take the longest to satisfy testing requirements.

[21] U.S. Department of Defense, *National Defense Industrial Strategy*, 20.

One issue is the chicken-and-egg problem: Companies need to have a contract to be eligible for most licenses and certifications, but they must have those licenses and certifications to receive a production contract in the first place.

How can the government assist companies in preparing for production without putting up new barriers for pilots?

One way would be to provide companies with a compliance checklist upon receiving a pilot contract. Venture capitalists set clear milestones for transitioning from one funding round to the next. A similar pathway consisting of clear milestones for companies maturing their technologies in the defense market does not exist. While companies bear primary responsibility for understanding their customers, the government can do more to help commercial companies understand the compliance requirements necessary to move from pilot to production so they can plan accordingly. Organizations sponsoring the pilot can work with program offices to provide a checklist consisting of the various compliance items companies need to satisfy to be eligible for production-level contracts.

Additionally, the *National Defense Industrial Strategy* recognizes that SBIR/STTR is a valuable gateway for many small businesses.[22] The Defense Department should further use this gateway by creating a category of supplemental SBIR/STTR funds for testing and evaluation. The SBIR/STTR program is a major source of initial government contracts, and thus the first exposure many smaller commercial companies have to government requirements. The government can hold some funding in reserve for "plus-up" of entry-level innovation contracts for testing and evaluation. The funds could be unlocked subject to a set of pre-defined requirements at award and would only be used for testing and evaluation for promising companies to go through certification processes, so that the government is better able to employ the solutions it is buying. These extensions could be executed through SBIR-trained contracting officers or a partnership intermediary agreement with access to relevant facilities.[23]

Intellectual Property Problems Abound

"DoD [struggles to understand] what a commercial sales model looks like, including private company IP rights."- Survey Respondent

Vague intellectual property rights language causes confusion between the Defense Department and companies, slowing award time and limiting the overall vendor pool.

Survey responses suggest that most companies would be willing to give up their intellectual property rights to the federal government. However, write-in responses add a degree of nuance, as most companies are deeply protective of their intellectual property and are wary of handing over their rights. This disconnect occurs because companies do not understand government intellectual property rights.

Among all respondents, 67 percent indicated they would accept language corresponding to government purpose rights on their contract, while just 24 percent would require restricted rights. Meanwhile, 27 percent of respondents are open to accepting unlimited rights on their contracts. Among venture capital-backed companies, 68 percent are open to either government-purpose or restricted rights, while only 15 percent are willing to accept unlimited rights. Companies do not understand the government's intellectual property rights framework. Accepting general purpose rights can seem harmless but can deeply impact a company's ability to profit within the defense market. On the other hand, the government either does not understand, or care about, company concerns about the need to protect their intellectual property. Companies develop products, and get funding for expansion, based on intellectual property and the defensibility of that intellectual property. However, the government requires access to the data to operate the system. Both parties — the company and the government — have an interest in reaching a mutually beneficial agreement on intellectual property rights.

Respondents highlighted that intellectual property rights negotiations are a common source of friction between companies and the government. One company representative explained that the "DoD [struggles to understand] what a commercial sales model looks

[22] U.S. Department of Defense, *National Defense Industrial Strategy*, 20.

[23] A partnership intermediary agreement is a contract, agreement, or memorandum of understanding with a non-profit partnership intermediary to engage academia and industry on behalf of the government to accelerate tech transfer and licensing. "Contracting Cone: Partnership Intermediary Agreement (15 USC §3715)," Defense Acquisition University, accessed January 19, 2024, https://aaf.dau.edu/aaf/contracting-cone/rd-agreements/pia/.

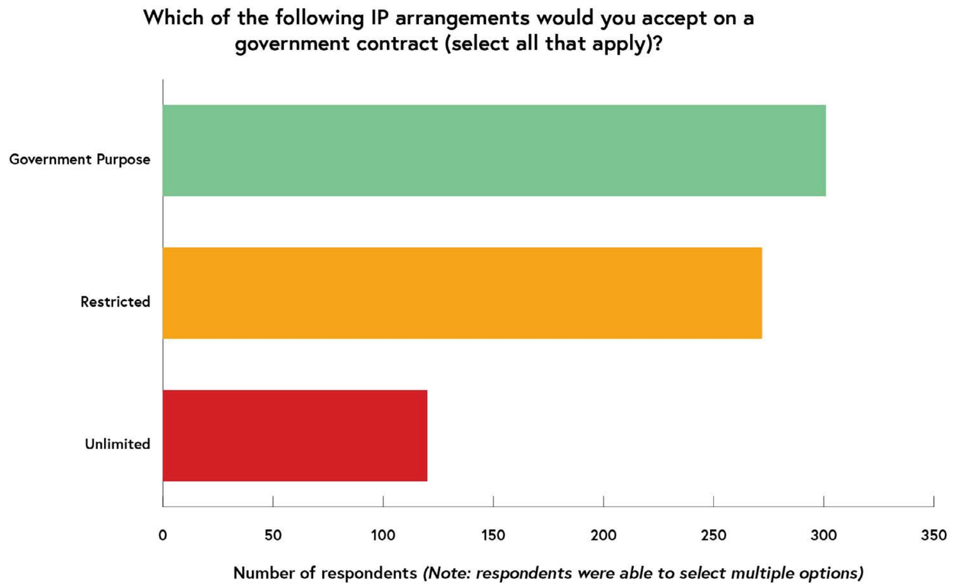

Figure 4. Intellectual Property

like, including private company intellectual property rights." Another added that "the [U.S. government] must do better at protecting our proprietary and SBIR rights." Others pointed to the disconnect between rights negotiated in SBIR awards, and those granted in follow-on contracts: "Getting SBIR data rights on contracts that extend from SBIR Phase I and II contracts [is a challenge]." Another explained that a contracting officer "has attempted to remove our existing data rights." A respondent summarized the difficult tradeoff that companies face: "The company either incurs significant fees to understand what they're agreeing to and negotiate with the government, or takes the risk, and neither is ideal."

Intellectual property rights negotiations should begin with a proven template based on previously accepted terms between similar companies and defense entities.

Negotiating intellectual property rights can be a daunting task for companies entering or growing within the federal market. The government often wants unnecessarily stringent intellectual property rights, either to minimize their perceived risk in the contract or due to differing perceptions of what they think they are buying versus what companies believe they are selling. Companies unfamiliar with the intellectual property rights process often struggle to weigh the costs of prolonged negotiations against the risk of accepting terms they fear they may come to regret. Such confusion results in companies either leaving the defense market with their technology or spending precious time and resources hiring an intellectual property lawyer. In both cases, the Defense Department loses because the underlying requirement remains unmet.

The *National Defense Industrial Strategy* acknowledges the challenges it has imposed on companies, stating that the Defense Department will "integrate IP planning fully into acquisition strategies" and "seek to acquire only those IP deliverables and license rights necessary to accomplish these strategies."[24]

There are two additional steps the Defense Department can take to reduce the friction around intellectual property rights. First, the government should create intellectual property rights templates for different business models to facilitate the transition from pilot to production. Most intellectual property issues surface as companies transition their capabilities and contracting moves from pilot to production. The government can clear the way for more companies to engage directly with fewer concerns and roadblocks by offering clearer guidance and standard frameworks. Intellectual property rights negotiations should begin with a proven template based on previously accepted terms between similar companies and defense entities. Doing so would ensure both parties are protected and reduce the time spent on negotiation. Such templates would give each party confidence and stability, while reducing the time to award and the cost incurred by small companies.

Second, the Defense Department should default to Other Transaction Authority for SBIR awards and check intellectual property rights for clarity and practicality. Government-published language is notoriously opaque and incomplete. As a result, some companies are too eager to do business without recognizing the risk, while others are scared away, believing the government will own their intellectual property. The Office of the Under Secretary of Defense for Acquisition and Sustainment should develop a plain-language communications document about intellectual property rights terms so companies can make decisions on their own, without involving lawyers. Federal Acquisition Regulation-based contracts present complicated intellectual property language barriers and outdated models of engagement that deter new entrants.[25] This is especially true for software, where the government struggles to differentiate between buying software licenses and buying services to develop software. Using Other Transaction Authority as a basis for SBIRs would provide better flexibility in negotiating rights in plain language as well as a baseline rights framework that can scale up to production.

Frozen Out by Classification

> *"We have huge value for classified activities (because most of them are supported by software engineering). Yet we can't make contact with clients without having clearance. And we can't get clearance without a classified client requesting it. We are stuck with an unsolvable problem."*
> *-Survey Respondent*

Dealing with classified information may be the greatest challenge companies face in accessing opportunities to work with the federal government.

Difficulties accessing classified environments prevent companies from entering the defense market. Classified environments frustrate the ability of companies to bid on new opportunities and deliver on existing contracts, insulating incumbents from competition even if they have inferior technology.

Among all respondents, 44 percent ranked accessing classified environments as the greatest barrier to working with the government, compared to 18 percent for obtaining necessary licensing and certifications, 15 percent for accessing test and evaluation facilities, and 14 percent for accessing data. The challenge of classification was greatest for companies whose leaders lacked government experience.

Respondents struggle with classified environments for two reasons: (1) gaining security clearances and (2) accessing cleared facilities. First, "getting security clearances for our team to meet and work in classified environments" remains a challenge for new entrants and small businesses, per one survey respondent. Obtaining security clearances is a problem because pilot contracts (especially SBIR/STTR) do not usually come with a Defense Department Contract Security Classification Specification (DD-254), which establishes the firm's need-to-know, and permission to do classified work.

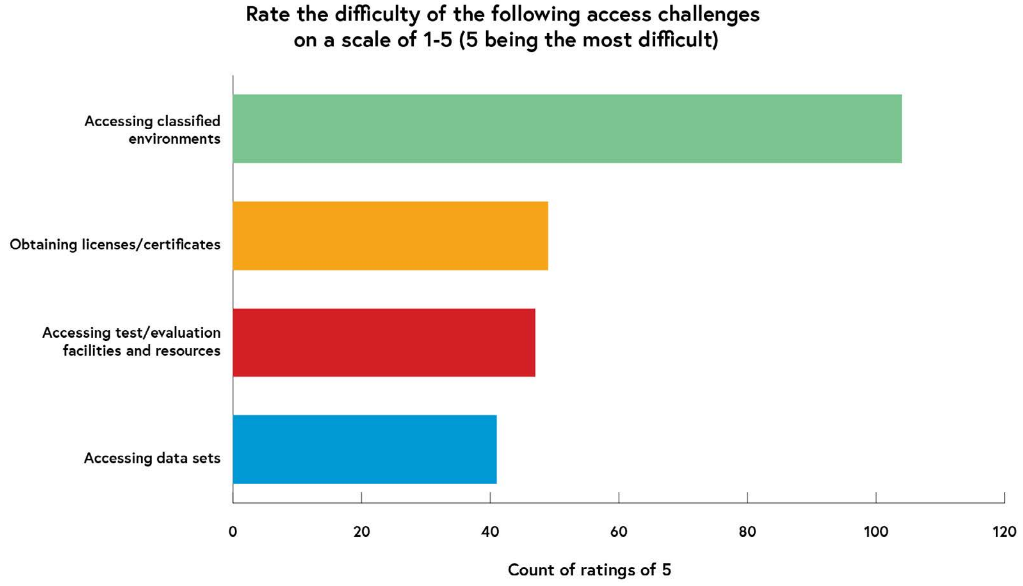

Figure 5. Access

[24] U.S. Department of Defense, *National Defense Industrial Strategy*, 37.

[25] The Federal Acquisition Regulation is the primary regulation used by executive agencies to acquire supplies and services with appropriated funds. "Federal Acquisition Regulation," U.S. General Services Administration, accessed January 19, 2024, https://www.acquisition.gov/browse/index/far.

Second, access to classified facilities is a problem, as small companies often lack the ability to perform work or learn about new opportunities in a secure facility. Multiple respondents reported difficulties gaining clearances for their facilities enabling them "to get classified communications at our facilities so we can respond to [request for proposals] and qualify for critical programs. Currently the vast majority of large [Defense Department] contractors have this access but the mid/small [-sized companies] do not." Another respondent pointed to the ways in which classification protects established contractors at the expense of newcomers: "It is often impossible to win without us using classified or [Controlled Unclassified Information] we have from other work, even on supposedly open competition." In short, many companies feel that they "cannot innovate if the door is literally locked shut."

A company lacking facility clearances or cleared personnel is often viewed as risky by the acquisition community. It is an easy argument for a contractor to disqualify a new vendor, or to stick with a trusted partner, even in the face of a superior technical assessment. As a result, large traditional prime contractors are insulated from competition, and the government limits its own exposure to new or commercial capabilities. To broaden participation in the defense industrial base, the U.S. government should solve the challenge of accessing classified facilities for qualified participants.

The government needs to find new ways to involve companies without security clearances into competitive bidding, rather than dismissing them out of hand.

The classification challenge goes unmentioned in the *National Defense Industrial Strategy*. There are a few immediate steps the Defense Department could take to help address this challenge. First, it could co-locate security officers, industrial security specialists, and security Defense Counterintelligence and Security Agency liaison officers within innovation units (e.g., AFWERX or the Defense Innovation Unit). There has been reluctance among innovation units to establish the need-to-know for companies, issue a DD-254, and begin the clearance process. As a result, many companies with pilot contracts do not have a realistic chance of deploying their products into the hands of end-users in classified environments, severely limiting the government's ability to leverage commercial technologies across the defense enterprise. An in-house security officer can begin to facilitate the clearance process while contracting work is ongoing, giving companies a better chance of success. The Defense Innovation Unit, as the front door to commercial companies, still relies on the Office of the Under Secretary of Defense for Research and Evaluation to process clearances, dramatically slowing the process. With a higher volume of contracts, and a smaller overall contract size, these innovation units are typically deprioritized and require a dedicated officer to prioritize their awardees.

Second, the Defense Department could use non-military sites to create secure compartmentalized information facilities (SCIF) for companies. One of the great challenges for companies entering the defense market is that even if they have cleared staff, those individuals require admittance to SCIFs to be able to access classified information, compared to traditional contractors who own and manage their own (expensive) classified facilities. This is a significant barrier for many companies on pilot contracts. The government should use the Mission Acceleration Centers, Defense Innovation Unit, and other off-base locations where companies can establish shared sites that provide SCIF access — either on existing contracts or for bidding on classified requirements. This may mean accelerating and scaling up the Defense Advanced Research Program Agency's Bringing Classified Innovation to Defense and Government Systems program to sponsor interim facility security clearances and giving companies access to classified terminals at select sites.[26] The government should also explore private company partnerships to make SCIFs more widely available.

One of the great challenges for companies entering the defense market is that even if they have cleared staff, those individuals require admittance to SCIFs to be able to access classified information, compared to traditional contractors who own and manage their own (expensive) classified facilities.

[26] "Bringing Classified Innovation to Defense and Government Systems," Defense Advanced Research Projects Agency, accessed January 19, 2024, https://www.darpa.mil/work-with-us/bringing-classified-innovation-to-defense-and-government-systems.

Conclusion

The Defense Department needs access to advanced commercial technologies to keep pace with adversaries. For this to happen, the department should build stronger partnerships with all types of companies. These partnerships should be mutually beneficial, allowing companies to swiftly discover defense customers while enabling defense customers to rapidly acquire commercial technologies. Otherwise, companies may lose interest and investors may lose patience and take their business elsewhere. A smaller vendor pool with less competition risks widening the defense technology gap between the United States and its technologically advanced adversaries. The potential harm to U.S. national security could be immense.

Over the past decade, Defense Department policies have focused on improving the government's ability to acquire commercial technologies. These policies have been highly successful at attracting companies to the defense market. The next step is to focus on the company side of the partnerships to improve the government's ability to retain company interest in the defense market by mitigating the issues they face. The outcome of an expanded supplier base should not be just an "increase in number of suppliers newly doing business with the Department," as the *National Defense Industrial Strategy* states.[27] Rather, the goal should be the rapid and widespread adoption of more advanced technology that is better able to accomplish essential mission objectives faster and more effectively.

Our survey results highlight five challenges that companies face when doing business with the U.S. government. These findings can help inform the development of new techniques the Defense Department can use to reduce these barriers.

Company success in the defense market is inextricably linked to the military's success on the battlefield. The government's success metric should not be tied to the success of any one company. Rather, success for the government means building the infrastructure that allows a parade of mission-driven entrepreneurs and company builders to develop, deliver, and scale disruptive technology and services to benefit the warfighter and strengthen U.S. national security. Achieving this goal means better aligning government policies and personnel with companies, making access easier, and eliminating the myriad obstacles that dissuade many from entering and thriving in the defense market.

Jeff Decker, *Ph.D. is managing director of Tech Transfer for Defense at Stanford University's Doerr School of Sustainability and is a co-instructor of the graduate-level Hacking for Defense course. Follow his work at Stanford's Hacking for Defense blog.*

Noah Sheinbaum *is the founder of Frontdoor Defense, a platform to simplify the defense industry for mission-aligned builders and operators. He also co-founded Defense Tech Jobs, a jobs board for defense technology companies, and consults for various purpose-driven companies.*

Acknowledgments: *The authors wish to acknowledge the contributions of the following experts and leaders for providing counsel and feedback on the survey and drafts of this article: Andy Bowne, Eric Blatt, Michael Breslin, Garrett Custons, Chase Eiserman, Daniel Gross, Brad Harrison, Sabrina Howell, Erika Hussey, Pete Modigliani, and Jonathan Mostowski.*

Image: *Navy Petty Officer 1st Class Alexander Kubitza*[28]

[27] U.S. Department of Defense, *National Defense Industrial Strategy*, 24.

[28] For the image, see https://www.defense.gov/News/Releases/Release/Article/3643326/dod-releases-first-ever-national-defense-industrial-strategy/.