Vol. 14, June 2018

MITCHELL INSTITUTE
Policy Papers

Key Points

In order to affordably operate, sustain, and modernize weapons systems, the Air Force needs access to more data than it has in the past. Both the Air Force and the defense industry must share an understanding of the critical role that intellectual property plays in the ability of defense suppliers to develop and maintain future technological superiority. At the same time the Air Force must take maximum advantage of those rights it precisely defines and procures to improve capability of weapons systems for decades to come.

While the government clearly has growing needs for procuring and using data, it also has a responsibility to meet those needs in ways that also encourage private investment and increase competition. Achieving this goal requires a mutually beneficial relationship between the Air Force and the broader defense industrial base that depends on both the continued competitiveness of traditional primes, their suppliers, and the ability to attract new commercial technology innovators to support the Air Force.

Each program will likely have different capability requirements and different lifecycle requirements. No acquisition is the same, and data rights should not be treated the same across those acquisitions. The Air Force must adapt their acquisition practices and workforce to address their increased need for data requirements and rights. These reforms should consider cultivating an acquisition cadre that specializes in data requirements and rights; developing a rational and rigorous process for identifying and defining data requirements and necessary lifecycle rights; and early and iterative discussions with industry during the RFI process.

Data Requirements and Rights: Time for a Reassessment

By Col Herbert C. Kemp, USAF (Ret.), PhD
Senior Visiting Fellow, Mitchell Institute for Aerospace Studies

with Maj Gen Lawrence Stutzriem, USAF (Ret.)
Director of Research, Mitchell Institute for Aerospace Studies

and Heather Penney
Senior Fellow, Mitchell Institute for Aerospace Studies

Abstract

Procuring military hardware in today's information age is a vastly different proposition than it was in decades past. But Air Force acquisition practices and preparation of its workforce have not sufficiently evolved to address the increasing importance of software in non-information technology procurement. There is not a consistent and rigorous approach to how data requirements and associated rights are developed, defined, and contracted to gain affordability across a program's lifecycle. Within this context, trend lines indicate a demand for more than is required.

The DFARS appropriately divides and defines the concept of data rights into two separate categories: technical data and computer software. The issue of data requirements is not just about what data is pursued; it is also about what kind of licensing rights the government seeks. For certain types of technical data, specifically operations, maintenance, installation, and training, the government is entitled to unlimited licensing rights. In contrast computer software data, the information and material that would allow the software to be reproduced, recreated, or recompiled, is not subject to similar compulsory unlimited licensing.

Aggressive and inconsistent pursuit of both technical and software data requirements and rights in recent acquisitions have only served to confuse the issue. Both the Air Force and the defense and commercial industry must share an understanding of the critical role that intellectual property plays in a thriving industrial base, access to innovation and competition, and ultimately technological superiority. Equally, both must clearly discern what access the Air Force requires to affordably sustain and modernize their weapons systems. A more rigorous and enforced derivation of requirements is needed. To do so, the Air Force should cultivate a cadre of acquisition officers who specialize in lifecycle data requirements and rights. Better government-industry dialog is needed to achieve the best outcome for the nation's greater, long-term interests.

Introduction

The Department of Defense (DOD), and particularly the US Air Force, are in the midst of a crucial transition: transforming a military that is largely a remnant of an industrial age whose value is based on hardware to that of an information-empowered force. While hardware and platforms will remain critical to solving the physical problem sets of range, altitude, speed, maneuverability, and payload, the relevance and effectiveness of these weapons systems are increasingly related to their information systems: sensors, software, networks, datalinks, fusion algorithms, and other factors. Air Force Lt Gen Lee Levy, commander of the Air Force Sustainment Center (AFSC), summarizes this shift: "Many of our weapons systems are simply software packages that come in a really nice, winged wrapper."[1] In other words, software is a growing driver in both the acquisition and the lifecycle of sustainment and modernization of Air Force weapons systems.

…procuring military hardware in today's information age is a vastly different proposition than it was in decades past. But DOD and Air Force acquisition practices have not sufficiently evolved to address the increasing importance of computer software content and source code in traditional procurement (non-information technology) programs.

Consequently, procuring military hardware in today's information age is a vastly different proposition than it was in decades past. But DOD and Air Force acquisition practices have not sufficiently evolved to address the increasing importance of computer software content and source code in traditional procurement (non-information technology) programs. There is not a coherent, consistent, or rigorous approach to how data requirements are developed and defined. That Air Force platforms are expected to remain in service for decades – in some cases, over fifty years – only further confound the data requirements problem. How can the service anticipate what data rights it will need in 40 years? Given Moore's Law (which states that computer chip processing power doubles roughly every two years) and the rapid cycle of software-based technological innovation, the data rights acquired in an initial program procurement will clearly have a lasting impact on the Air Force's long-term options to modernize and sustain these platforms.

The Defense Federal Acquisition Regulations Supplement (DFARS), the guidelines that dictate DOD acquisition practices, limit government acquisition of data rights to: "…only the technical data, and the rights in that data, necessary to satisfy agency needs…" and requires the government acquisition manager to "…address acquisition strategies that provide for technical data and the associated license rights…" required from the program.[2] That is, by regulation, the acquisition strategy should seek to identify the data rights required across the life of the program, and its acquisition strategy should secure only those rights, and no more. This approach would ideally prevent the service from paying more for what it does not need, and also balance the interests of industry to preserve appropriate intellectual property (IP).

Despite the DFARS guidance, there is no real clarity regarding how to define data requirements. Unlike platform performance requirements that follow an established process to generate and justify key performance parameters and other such requirements, there is nothing codified on how to define what data rights are necessary for the government to acquire. Without a deliberate process to guide acquisition program offices on how to assess what data will be required over the lifespan of the program, each individual office appears to have a different take on data requirements and the associated licenses and rights. That is, each program executive officer (PEO) is left to develop their own "best practice." This has resulted in very different philosophies regarding how to untangle the thorny issue of lifecycle data requirements, and appears to have encouraged a certain amount of overreach when it comes to procuring data rights in recent acquisition programs.

But what is required? What data rights will be necessary and sufficient to "satisfy agency needs"? The Air Force seeks to maintain, sustain, and modernize their hardware and software in the most effective, efficient fashion possible. Adequately identifying the data requirements for the lifecycle of the program and procuring the necessary data rights are key to this goal. That is why the Air Force is leery of "vendor lock," when a single company (typically the original equipment manufacturer, or the OEM) controls the hardware and software in question; data rights can be a mechanism for such

control. An OEM that wields the power of what is essentially a monopoly can, from the government's perspective, hold the program "hostage." While the initial down-select spurs competition, once a program award is made, the Air Force can find itself bound to the OEM as the only company with sufficient knowledge and access to maintain and modernize the program.

For a service that now operates major weapon systems for decades, the information technology systems that make those weapons systems operationally effective will face rapid obsolescence. Will an OEM always have the most innovative solutions? Will they always be the best partner to quickly field new software or technologies? One Air Force acquisition handbook states "…the program office should acquire sufficient rights so it will not need the original equipment manufacturer, or OEM, to maintain or sustain the system."[3]

Under the DFARS and 10 USC 2320, the US government is only to order data which meets a minimum and identifiable need, and for that ordered data, cannot force contractors to give up their data rights or refrain from offering privately developed technologies due to data rights.

It is important to note that sustainment is not simply about a spare parts warehouse; capability modernization and upgrading is an increasingly important aspect of the sustainment lifecycle, and is not limited to computer software. Indeed, software and hardware are increasingly linked and integral to the other's efficacy. Within this context, it does not seem unreasonable that instead of limiting their appetite for data requirements and the subsequent data rights, trend lines in recent acquisition programs indicate a much broader sweep by the Air Force—one that is alarming the defense industry and their supply chain.

The Air Force wants liberal access to data rights to sustain, upgrade, and evolve systems independently from whomever may have developed the original technology. Said quite simply, the service wants to avoid vendor lock on programs and preserve their options for the future. While these objectives are quite rational, it becomes problematic when the services seek to acquire data and rights beyond the DFARS, which implements 10 USC 2320. Under the DFARS and 10 USC 2320, the US government is only to order data which meets a minimum and identifiable need, and for that ordered data, cannot force contractors to give up their data rights or refrain from offering privately developed technologies due to data rights. Over-ordering data is not an appropriate insurance policy; it is against DFARS policy. Acquiring more data than the US government needs, as well as requiring contractors to give up data rights protections or refrain from offering data with restrictions are both violations of the DFARS data scheme. Furthermore, recent behavior by the Air Force indicates that the service may indiscriminately flow their demands for data requirements and data rights down through the entire supply chain. As a result, Requests for Proposals (RFPs) may include requirements to provide unlimited or government purpose data rights for technologies whose development have been funded with resources independent of the DOD, which is contrary to the DFARS and which may not be controlled by the prime contractors.

As momentum within DOD to acquire data and data rights has grown, recent solicitations reveal that the service may be overreaching without considering the holistic nature of data requirements and rights. Instead of securing only the necessary data rights needed to facilitate lifecycle requirements in a flexible, forward-leaning fashion, recent RFPs suggest the US military services may be pursuing a "big grab" approach by demanding vast swaths of information. The data requirements expressed in the RFPs may extend far past actual pragmatic needs and statutory guidance, especially when it comes to software source code for vendors and sub-vendors.

Indeed, the expanding US government focus on software requirements and rights parallels the expansion of software in terms of total program content. But such data requirements risk increasing cost, reducing competition, and stifling innovation. An offeror would need to price in the cost of purchasing data from their entire supply chain (if their vendors agree to do so), resulting in a higher program cost. Firms may choose not to participate in future acquisitions, or defense primes may need to acquire small businesses in order to satisfy the government's demands for the data (thereby decreasing competition). And any company, be they large or small, will not surrender

their foundational intellectual property to sell a couple dozen assets to DOD, especially when they may be retailing much larger quantities for much higher profit margins in the commercial marketplace. Ironically, the actions the DOD is taking in pursuing data risks their other acquisition goals of decreasing cost, leveraging commercial technology, cultivating small businesses, increasing competition, and incentivizing innovation by driving commercial companies away.

However, the concerns of the DOD that are driving its appetite for data rights are real and reasonable. Addressing data requirements and data rights in a balanced way represents a major issue for both government and industry, and a critical one to solve. Instead of an "all or nothing" approach, the real solution comes down to a far more nuanced approach that will allow both government and industry to benefit from carefully derived and defined data requirements that reflect contemporary dynamics. Better policy, process, and training is needed for determining the actual data rights the government needs to achieve desired effects. To this end, the US government and private industry must collaborate to establish acquisition strategies that respect DOD concerns, while also working to provide a common understanding of fair and proper compensation for data rights, improve requirements definition needed for realistic pricing methodologies, better define end use parameters, and enhance protections for proprietary information.

Data requirements and rights in defense acquisition are an esoteric and complex subject, and are worth a baseline review. At a macro level, technical data is the intellectual underpinning on which goods and services are created.

Understanding Data Requirements and Data Rights

Data requirements and rights in defense acquisition are an esoteric and complex subject, and are worth a baseline review. At a macro level, technical data is the intellectual underpinning on which goods and services are created. It all comes down to the essential pieces of information that explain how to operate a program or capability, repair it, and install it, or even how it was made. This technical data might take the form of an instruction manual, physical blueprints and specifications for a piece of hardware. When required under a contract, the technical data is delivered with associated licenses (i.e., data rights) that discern what the government can do with the delivered data. Rights specifically refer to the privileges associated with the type of license procured, and therefore the term is broadly used to discuss the larger issue of data licenses.

When the DOD acquires a product, the technical data rights that they are privileged to, and limited from, are spelled out in the DFARS. Specifically, the DFARS, interpreting 10 USC 2320, provides the DOD unlimited rights to what is referred to colloquially as "OMIT data": data necessary for operations, maintenance, installation, and training (other than detailed manufacturing or process data, including such data pertaining to a major system component).[4] The US government is not automatically entitled to anything above and beyond this OMIT data, and access to that data must be negotiated through license (data rights) procurement.

OMIT data is typically contained in technical orders (TOs). For example, operations technical data are necessary for the military to understand how to use and operate the article. There are several levels of maintenance data, depending on the complexity and depth: these include basic frontline maintenance and servicing, repair, "back shop," and depot-level activities. Installation data describes the required support equipment and building or facility requirements, and training includes all the information and data necessary to teach all special instruction involved with the program. In order to be unlimited rights, OMIT data, under the DFARS, does not include detailed manufacturing or process information that would enable the government or any third party to replicate the way in which it functions, or build the whole or any part of the whole. OMIT data also specifically excludes computer software and source code.

A common example can be helpful in understanding, by way of examining consumer products. When a consumer acquires a product, whether it be a physical item or software, it is important to understand that they are generally not procuring all the data rights, as well as all

the data, for the commodity. In one obvious case, when a consumer buys an automobile, they acquire the hardware and software of the automobile. The operations technical data (owner's manual) is in the glove box, as well as the basic maintenance data (usually as a supplement to the owner's manual). And beyond the basic maintenance manual, more detailed technical information is also provided to allow technicians to repair the vehicle (both at the dealer and any local garage). Installation information is not generally provided, as vehicle dimensions are fairly standard for garages and street parking and gas stations are prolific, but installation data for hybrid or fully electric vehicles (what kind of power source and cable) would be included. Finally, the salesperson provides training to the new buyer, showing them how to operate the radios, navigation packages, touch screens, and so forth. However, the manufacturer does not give the consumer proprietary information tied to the design and construction of the car—what would be manufacturing and process data, such as blueprints. Source code to reprogram the car, from the navigation and software package to engine management or fuel economy logic, is not provided either. This intellectual property, developed by the manufacturer, remains their property, and constitutes the basis for their competitive market position. The only exceptions to this practice would be if an individual funded the development of a new car and negotiated for the data to be delivered with associated licenses and rights as part of the purchase or if the intellectual property information was procured through an additive transaction.

Automobiles, and many other consumer goods, are no longer just defined by hardware; software matters as much, if not more. Repairs typically require a trip to a mechanic because the technology and software exceed the owner's expertise, and the owner does not have access to the proprietary code in the car.

Any car owner who grew up operating a manual transmission and carburetor knows how different and sophisticated today's vehicles are compared to those produced just a few decades ago. Much of a car's performance is wholly dependent on its software. While these technological and software advancements have led to vehicles with exquisite performance, it can be frustrating and expensive for owners who are no longer able to work on their own car in their own garage. Automobiles, and many other consumer goods, are no longer just defined by hardware; software matters as much, if not more. Repairs typically require a trip to a mechanic because the technology and software exceed the owner's expertise, and the owner does not have access to the proprietary code in the car. Even the local mechanic may not have the required data or program source code to complete the repair, and a car owner must take the automobile back to the dealership. This is the situation the DOD increasingly finds themselves in: software is an increasingly critical piece of combat hardware, but computer software is treated differently than technical data for hardware under the DFARS. This is largely because software "maintenance" involves modifying the software to create a new program, whereas hardware maintenance using OMIT data returns the broken hardware to its original operational state.[5]

However, returning to the example of a new car buyer who also owns a 1957 Ford Thunderbird (the same production vintage as the B-52 Stratofortress, which ran from 1952 to 1962, it should be noted), the sustainment and maintenance problems inherent in all vehicles are not just about the sophistication of software. Old cars and old airplanes share a similar challenge when it comes to sustainment: diminishing manufacturing sources (DMS). Even when the original manufacturing company is still in business, technology and the market have moved on. Parts become hard to find. Access to manufacturing and process data (blueprints) are the only way to build replacement parts once old stocks are exhausted. Given the unexpected and unprecedented duration of service that the Air Force finds itself extending its aircraft, diminishing manufacturing sources is a very real challenge. Additionally, in order to modernize these weapon systems over their lifecycle, the service requires detailed technical data to integrate new capabilities. This brings us back to our automobile analogy—how else would a 1957 Thunderbird owner install anti-lock braking, a satellite radio, or self-driving capability, without access to detailed technical data?

While often grouped together, the DFARS appropriately divides and defines the concept

of data rights into two separate categories: 'technical data' and 'computer software' delivered by contractors under civilian agency and DOD contracts.[6]

Technical data: Technical data generally includes any information contained within computer databases, product design, documentation, specifications, and maintenance material.[7] Simply put, technical data can range from something as simple as the maximum torque used to tighten a particular bolt, to something as complex as the detailed procedures to dismantle and overhaul some intricate subsystem of an aircraft, like an aircraft engine.

Computer software: Software, on the other hand, excludes computer databases and computer software documentation, but includes "…executable code, source code, code listings, design details, flow charts, and related material that would enable the software to be reproduced, recreated, or recompiled…"[8] This delineation is important because computer software is explicitly not technical data, and therefore not subject to the automatic access and unlimited rights that OMIT data is subject, whereas computer software documentation (i.e., user manuals) are subject to unlimited rights.

The type of rights the government receives in non-OMIT data is usually governed by how the development was funded.

Again, to use a more familiar example, when a consumer buys a commercial application to run on a home computer, the consumer acquires the rights to use the software for any legal purpose. However, the consumer does not necessarily acquire the rights to rewrite, copy, reverse engineer, or modify the underlying code. Underlying code, or source code, is important to the US government as it seeks to sustain weapon systems over time. The challenge this poses is that just like software maintenance (which typically involves "debugging"), modifying code for upgrades essentially creates what is essentially a new software program. Since changes to the software as part of any sustainment process necessarily makes the program behave differently, it poses very different risks to the warfighter and needs to be well regulated and understood to prevent unintended consequences.

Finally, the issue of data requirements is not just about what data is pursued; it is also about what kind of licensing DOD seeks, what is also referred to as data rights. OMIT data, by default, is always granted to the government in the form of unlimited rights.

The type of rights the government receives in non-OMIT data is usually governed by how the development was funded. The DOD may have unlimited rights for data which was developed entirely with federal funds; government purpose rights in cases where both government and private funds have been used in development; and restricted or limited rights for cases in which the service negotiates specific data rights with respect to "…items, components, or processes developed exclusively at private expense…"[9] Unlimited rights are the most liberal, conferring to the government the ability to "use, modify, reproduce, release or disclose technical data or computer software in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so."[10] However, it should be noted that under current DFARS rules, technical data is protected under Government Purpose Rights for only five years, after which it is reclassified under Unlimited Rights. This timeline is much more aggressive than would normally be the case in the private sector and shortens the period in which industry must recoup its IP investments in a given technology product.

In summary, the types of rights the US government has in licensing will also have a significant impact on their ability to sustain a weapons system over the course of its service life. These distinctions further complicate the issue of data requirements and rights, given the increased shift towards incorporating commercial items and software into defense programs. Data associated with commercial items – whether technical or computer software – falls under restricted or limited rights.

The use of commercial technology is both lucrative for the government and presents a clear challenge to current trends. Recognizing the potential advantages of the speed of commercial development and modernization; unit cost amortization; and the research and development (R&D) offset of harnessing commercial industry's innovations, DOD has made a deliberate decision to leverage the power of American commercial

industry in its acquisition practices.[11] Moreover, DOD incentivizes civilian innovation for defense-specific (non-commercial) technologies using mechanisms such as reimbursable independent research and development (also known as IR&D). Frankly speaking, harnessing civilian innovations can provide cheaper and faster solutions for the DOD, and can be done while still allowing contractors to protect their data with increased restrictions on the US government's taking of privately developed technology.

But as with all things related to the US government, this is not that simple or easy.

Military acquisition is still a military-specific enterprise, and very rarely are solutions purely commercial products. More often than not, commercial components are leveraged by the defense industry to increase the capability and reduce the cost, time, or complexity of a dedicated military system.

This is today's gray area of data rights: In a world where the DOD is encouraging increased use of commercial hardware and software to be integrated in military purpose-built products that will endure for decades, what is the appropriate balance of technical data, computer software, and the scope of US government rights? The answer is somewhat easy if the development and production of the program is wholly funded by the DOD. Data rights are likewise obvious if the product is very clearly a commercial article, or where the data pertains to privately developed technology. But when the program is military-purpose, funded by DOD but incorporating numerous commercial hardware and software elements, data rights management becomes extremely problematic.

Military acquisition is still a military-specific enterprise, and very rarely are solutions purely commercial products.

Commercial firms are very careful regarding how they manage their company's data rights. After all, their proprietary designs, methods, processes and software code are the essence of their value as a company—it is how these firms stay in business. When companies commit their own funds (or reimbursable IR&D funds) in developing products, they expect to earn a reasonable return on those investments. Companies that share access to their data rights reasonably expect and must trust that their partner will safeguard the information in question. Otherwise, they risk a severe breach of proprietary interests. Defense industry prime contractors must act to protect both their proprietary information and that of their commercial supply chain. While much of the development, integration, and production work accomplished by prime defense contractors fall under federal funding, many of their subcontracted suppliers are commercial entities, or are firms that have invested IR&D to create the product. When data rights and requirements go deep into a supply chain, this risks the proprietary competitive value of the commercial company participating in the contract, and increases cost to the program. Even worse, it could pose a financial liability to the contractor team.

The challenge for both private industry and the government becomes one of operating under a set of rules that empowers industry to innovate and succeed, while also allowing the DOD to secure necessary and sufficient access to data, with rights for prudent force management and modernization. Those rules are governed by acquisition law and are codified in DOD acquisition regulations. Privileging the needs of one side over the other may be a short-term win, but will hurt the government-private sector partnership in the long run.

In remarks made this past May, AFSC's Lt Gen Levy acknowledges the tension between the drive for cost and the need to husband the industrial base, by noting that if it is not careful dealing with this problem set, the US government could make "cost per flying hour decisions that are operationally deleterious…. that disenfranchise the industrial base and drives it out of the marketplace."[12] The exact specificity of data requirements and license rights, plus their scale and scope, are essential to smartly balancing industry, commercial, and government interests for the long run.

Policy, Legal, and Regulatory Framework

While data rights-related challenges have always existed in defense acquisition efforts, the scale and scope of the issue is rapidly expanding as modern weapon systems reflect the software-centric nature of the information age. As explained in several Government Accountability Office (GAO) reports, the Department of Defense has

often struggled to identify what specific data rights are needed to sustain programs over the duration of their lifecycle. This is despite requirements in statute and policy that specifically require this planning.[13]

Late recognition (post-contract award) by the US military services can dramatically increase the costs of acquiring the necessary rights. A 2002 study cited one instance in which a government program office tried to procure data rights post contract award and was quoted a price nearly equal to the acquisition of the original program.[14] Similarly, a 2006 report found that the US government's failure to procure appropriate technical data rights at the beginning of certain programs drove sustainment problems for seven Army and Air Force programs.[15] A 2014 effort highlighted additional problems in this regard.[16] Acquiring the appropriate data rights during initial contract award is the most cost effective solution for the US government, and sets the right relationship between the contractor and the government.

Acquiring the appropriate data rights during initial contract award is the most cost effective solution for the US government, and sets the right relationship between the contractor and the government.

Because the timing of securing necessary licenses is so critical to the US government, new language in 10 U.S. Code § 2439 contains a specific focus on data rights by directing that:

> *The Secretary of Defense shall ensure that the Department of Defense, before selecting a contractor for the engineering and manufacturing of a major weapon system, or for the production of a major weapon system, negotiates a price for the technical data to be delivered under the contract for such development and production.*[17]

This clause seems to further propel the recent trend of broad reach of data requirements and rights in Air Force acquisitions. And as mentioned, lifecycle data rights are a major issue given the lengthy service of most major weapon systems, and negotiating those terms up front is crucial to service needs. But the assumption behind this clause is that data requirements and the type of licensing are reasonable, and have undergone a rigorous process for determining what is appropriate and necessary to support sustainment and modernization over the span of the program. Furthermore, each offering in a competition may be sufficiently different in software and commercial content that there is no reasonable methodology to compare offerors during the evaluation process. Well intended, this language appears to be putting the cart before the horse.

In 2009, Congress passed the Weapon System Acquisition Reform Act (WSARA) to foster greater competition. Two provisions of this law are relevant to data rights: 1) "Use of modular, open architectures to enable competition for upgrades" and 2) "Acquisition of complete technical data packages."[18] The first provision is relevant to the data rights discussion since the entire notion of modular technology is based upon seamless "plug and play" capability. In many ways, modular, open architectures mitigate a number of software modernization concerns because they do not require the OEM to provide fully integrated software. Systems are designed to integrate to common standards, which helps limit exclusive proprietary standards.

Acquisition of so-called "complete technical data packages" is a thornier clause. Data packages are important because they include specifications necessary for downstream sustainment efforts. But what does "complete" mean, in reality? Is it simply what is necessary and sufficient to sustain the program across its lifecycle and no more? Is the "complete technical data package" that which is defined and limited by statue? According to the MIL-STD-31000A guidelines, which apply to all DOD organizations, a technical data package contains, "…models, drawings, associated lists, specifications, standards, quality assurance provisions, software documentation, packaging data."[19] It is important to note that software documentation does not equal software code.

In 2016, the National Defense Authorization Act (NDAA) recognized the increased friction and complexity that data rights were posing to both the DOD and private industry. The result was the creation of the "Section 813 Panel" (named for the section of the NDAA in which it was directed), officially known as the Government-Industry Advisory Panel to review and make

recommendations regarding 10 USC 2320 and 2321—the statutes which govern "rights in technical data and the validation of proprietary data restriction." The legislative language reflected the balance of competing interests, directing the panel to give consideration to ensuring that the DOD did not pay multiple times for the same work; had affordable options across the lifecycle of a weapons system; had access to commercial technologies; and accounted for modular open system approaches. Likewise, the panel needed to provide recommendations that would appropriately reward and compensate companies for their IP and encourage private sector investment in research and development, as well as profit investments by traditional defense firms. Subsequently, the 2017 NDAA, Section 805, added a requirement for a modular open approach for all major weapon systems receiving Milestone A (material solution analysis) or Milestone B (technology maturation and risk reduction) approvals after January 1, 2019.[20]

Under the DFARS, licenses for technical data and computer software are distinctly different and are subject to different sets of rules. As noted in one analysis, recent Air Force actions appear to be on a path to conflate the two and constitute overreach beyond the limits of the authorities stipulated in the DFARS.

More recently, language proposed by the US Senate would have included computer software within the statutory definition of technical data; however, the final language in the FY 18 NDAA rejected this inclusion. Still, the progression toward greater US government interest in software used by and in national defense programs appears to be accelerating.[21] The issue of defining technical data and its use by the US government is not going away. The Defense Innovation Board (DIB) has recently released a draft of its so-called "Ten Commandments for Software," with commandment six recommending including source code as a deliverable for all purpose-built DOD software, citing such issues as security, performance and rapid deployment of upgrades.

Not everyone in DOD acquisitions agrees with this approach. For example, Dr. William LaPlante, former Assistant Secretary of the Air Force for Acquisition, said that overall "government should avoid source code – it's not practical, not a good idea."[22] Simply put, the US government should not be in the software business. Software development is a fast moving, innovative field of endeavor and what is important is what is called a "software factory," and making sure that industry and government keep the software robust over the life of the program.

The DIB's commandment number seven from its draft guidelines build on number six, recommending embedding a local team of DOD software experts in modern weapons programs to make rapid upgrades to software, through either source code access for DOD custom-built software or application programming interface (API) for other software.[23] LaPlante suggested that a better path may be the implementation of the "continuous iterative development" of software suggested by the Defense Science Board (DSB).[24] This would best be achieved by private sector software developers either responding to government requirements, or by private sector software developers offering new innovative techniques and capabilities to government.

Even without such revisions, new US government interpretations of the DFARS are blurring the lines between technical data rights and computer software rights. Under the DFARS, licenses for technical data and computer software are distinctly different and are subject to different sets of rules. As noted in one analysis, recent Air Force actions appear to be on a path to conflate the two and constitute overreach beyond the limits of the authorities stipulated in the DFARS. Under OMIT "…the Government obtains unlimited rights regardless of contractor development at private expense."[25] And while OMIT data (and its associated unlimited rights) is open for some interpretation because it is not specifically defined in law, it is explicitly clear what OMIT does not encompass: software. OMIT data is technical data for purposes of data rights; and because computer software is, by statute definition, *not* technical data, the unlimited rights of OMIT data do not confer to computer software: "computer software is not OMIT data, because software, also by statutory and regulatory definition, is not technical data, and, under 10 USCA § 2320, OMIT unlimited rights apply only to technical data." Case law strengthens the argument that

this kind of overreach, assuming unlimited rights in software through OMIT, is against legal precedent and constitutes a subtle interpretation of data rights. This does not mean that the service's concerns regarding life cycle management and modernization are invalid, but that the current approach taken by the Air Force with respect to data rights is troubling and problematic.[26]

Why is this important? Software source code represents competitive advantage for innovative technology companies—both commercial and traditional defense companies. Source code provides the programming instructions that make software function; it is the "secret sauce" that delivers a program's capability and constitutes the most closely guarded proprietary information in an information technology driven system. By including software code within the definition of OMIT in an attempt to obtain unlimited rights in source code, the Air Force effectively negates a company's competitive advantage by exposing their proprietary data or intellectual property and improperly interprets the statutory term in the context of computer software. This is not likely to encourage innovation or to attract cutting edge technology companies to do business with the US government. It is for this reason that LaPlante believes in the importance of non-proprietary modular interfaces, and argues that software development inside each module can be where industry innovates.[27]

Software source code represents competitive advantage for innovative technology companies—both commercial and traditional defense companies. Source code provides the programming instructions that make software function; it is the "secret sauce" that delivers a program's capability and constitutes the most closely guarded proprietary information in an information technology driven system.

Through specific legislative efforts, the government acquisition community has also sought to reward offerors for their willingness to provide data rights in excess of those required by statute. Although acquisition officials may not require an offeror to provide data rights past those authorized by statute (10 U.S.C. § 2320(a)(2)(F), the US government is not prohibited from accepting offers that afford more access in this lane. In other words, the DOD could incentivize offerors to surrender their data rights through a best value or full trade-off competition.

Ironically, all these trends in technical data and software rights run counter to the intent and purpose of DOD's headline acquisition initiative, Better Buying Power 3.0 (BBP 3.0).[28] BBP 3.0 is the third instantiation of this DOD-wide effort to improve defense acquisition practices, its headline being: "Achieving Dominant Capabilities through Technical Excellence and Innovation." There are a number of tenets under this effort. While the following list is by no means all-inclusive, it includes lines of efforts such as "Achieving Dominant Capabilities While Controlling Lifecycle Costs;" "Incentivizing Productivity in Industry and Government;" "Incentivizing Innovation in Industry and Government;" and "Promote Effective Competition." The nuts and bolts of data requirements and data rights lie squarely within the themes that BBP 3.0 focuses on. Included is the imperative to "remove barriers to commercial technology utilization," with emphasis upon the need for technological refresh rates as a key driver for change. Furthermore, BBP 3.0 specifically ties this goal to leveraging the technological innovation often seen in small technology companies. [29]

Owning the technical baseline (OTB) is a relatively recent approach to the acquisition of complex weapon systems and was first piloted across a number of major acquisition programs beginning in 2015. OTB follows established authorities in government technical data rights and is aligned to the "innovation and technology focus" of BBP 3.0.[30] Owning the technical baseline does not necessarily mean owning all the data, nor does it entail unlimited rights to that technical data or software code. The focus of OTB is to ensure that the acquisition organization has the engineering competencies, sufficient access to engineering data, and engineering analytic tools and capabilities to understand, assess and direct the program. Technical baselines are "product descriptions of functions, performance, and interfaces" and are closely associated with project work break down structures. They are supported by technical data packages as described earlier, but do not include access to computer software.[31]

Commercial companies are less likely to provide data or non-commercial data rights for their best products to the US government, and may not be within the competitive window as a result. These firms simply cannot afford to cede important proprietary information that ties to their future success. Small technology companies are even less likely to take this risk. This is especially true for dual-use civilian-military technology, where a firm will often sell more products on the private market than to the government. If DOD wants to attract top-tier talent, it needs to understand that it is not always a given company's biggest customer. Broader market forces will drive beneficial innovation and pricing, and run counter to the DOD's desire to leverage commercial companies and their technology.

All of the major prime defense contractors are heavily reliant on lower tier suppliers for the systems and subsystems comprising their major platforms. Many of these suppliers are small businesses with limited product ranges that are sold for use in both military and civil aircraft. These suppliers provide the gamut of subsystems and components ranging from electrical switches, avionics, and multi-function displays to servos, cables, and landing gear components. Component suppliers are reliant on their own IP protection for their future innovation and future business. The potential departure of such firms from the defense market would decrease competition within the supplier base and would require prime contractors to qualify new suppliers from a more limited pool. Since many of these suppliers are also small businesses, to the extent that the defense market becomes unattractive, the government's small business goals will become that much more difficult to achieve.

…if DOD continues to apply pressure, the primes may seek to simply acquire smaller commercial suppliers to limit the continued financial exposure posed by the new appetite for data and software rights.

For traditional defense firms, the lower amounts awarded in a value adjusted, total evaluated price approach are very unlikely to offset the inherent program costs of purchasing the full technical data and software rights from their suppliers. As a result, primes are incentivized to pursue less capable (and therefore less costly) commercial technologies—not necessarily the best technologies. These acquisitions might include older and outdated technologies that are no longer commercially proprietary. Finally, if DOD continues to apply pressure, the primes may seek to simply acquire smaller commercial suppliers to limit the continued financial exposure posed by the new appetite for data and software rights. The unintended consequence is that instead of increasing competition, these DOD policies might actually decrease the competitive field and number of DOD-qualified small businesses.

In sum, these trends all tie back to the need for better dialogue and a more nuanced and tailored approach to the subject of data requirements and data rights.

Air Force Approach to Data Requirements and Rights in Major Programs

A sampling of the Air Force's current major acquisition competitions can be illustrative regarding the trend lines in data requirements definition and the types of rights sought. This review is not intended to be an exhaustive analysis of ongoing solicitations, as that is beyond the scope of this paper. However, a sampling of the Air Force's respective approach to data requirements and rights reveals a varied approach to the issue, whether applied to aircraft programs, space assets, or non-flying weapons systems.

The broad reach for requirements and liberal data and software rights is perhaps most dramatically demonstrated in recent Air Force aircraft programs. As previously mentioned, many of these platforms are now operating at the end of unprecedented service lives. For example, the B-52 is projected to remain in combat service for 100 years since it first entered the inventory—a century of service for a single aircraft. Fighter aircraft, like the F-15 and F-35, are on track to be in service for over 60 years. Sustainment and modernization are of paramount importance to the Air Force's aircraft portfolio. As a result, there is a real interest in acquiring greater accessibility to the technical data and computer software.

In many ways, these programs reflect DOD's evolution from the industrial age to the information age. Aircraft like the F-16, F-15E, and B-2 came of age in the 1980s and 1990s, the exact same period when computing power, sensor technology, and

connectivity ramped up in an exponential fashion. Software and advanced processing capability took on a whole new level of importance, turning mere airplanes into weapons systems with unlimited capability growth potential. Defense firms were aggressively innovating, developing new solutions that were pioneering into realms of capability never previously explored. This meant their offerings were highly proprietary in nature, and government acquisition officials did not always understand the full implications of the systems they were procuring; and they certainly did not anticipate the unprecedented and unplanned duration of service. The result was an incomplete understanding of lifecycle considerations.

Today, both government and industry have a far more robust understanding of how the advancements in software, integration of capabilities, and the speed of technology impact long-term modernization and sustainment. While it may be too expensive and time intensive to redesign the core systems of weapons systems that are already fielded, the Air Force and industry now have a perfect opportunity to get the current generation of acquisition far better aligned for both parties.[32] Leveraging the affordability and effectiveness of proven designs, developing advanced new designs, and merging leading edge commercial technology means that every new program will be a blend of commercial, traditional defense, mature technology, and military-specific, purpose-built platforms. One size cannot fit all in this environment. This is exactly why data requirements and rights are such a crucial issue.[33] While the platforms themselves may differ, the underlying themes regarding data rights are what count. That there is variance in the Air Force approach to data and software rights demonstrates that there is room to develop a more deliberately tailored approach to each program, service needs, and industry interests. It is therefore instructive to examine some of these programs more closely.

The UH-1N replacement request for proposals (RFP) includes a special contract requirement that defines OMIT to encompass both technical data and computer software, and asserts rights to such data for both prime contractors, their suppliers, and subcontractors.

The UH-1N Helicopter Replacement Program

This Air Force competition aims to acquire 84 helicopters to replace the Air Force's remaining Vietnam-era UH-1N. These helicopters evacuate congressional and executive branch leadership in national emergencies, fly other VIP transport requirements, and support security requirements for nuclear missile personnel.

Three companies are in contention: Boeing/Leonardo proposed their MH-139 helicopter, a militarized version of Leonardo's AW139 commercial helicopter. Lockheed/Sikorsky proposed their HH-60U helicopter, the latest variant of the HH-60 Blackhawk helicopters built for military use.[34] The Sierra Nevada Corporation is also offering a refurbished UH60L with a Garmin avionics suite. The differences between the commercial-modified Boeing/Leonardo MH-139, the HH-60 Blackhawk offered by Lockheed/Sikorsky, and the Sierra Nevada offerings clearly illustrate why a one-size fits all data rights approach is simply not functional for today's acquisition environment.

The UH-1N replacement request for proposals (RFP) includes a special contract requirement that defines OMIT to encompass both technical data and computer software, and asserts rights to such data for both prime contractors, their suppliers, and subcontractors.[35] The flow-down of these requirements and data and software rights to suppliers and subcontractors is potentially problematic in a program of this size, which may well involve hundreds of lower tier vendors. The primes are offering mature aircraft with established supply chains and/or significant commercial content. This clause imposes significant cost on any competitor, who must purchase the data and software packages and data rights from their suppliers or assume associated financial liability.

This Air Force solicitation also requires that the chief executive officer of any prime contractor making an offer certify that the submitted proposal meets all the RFP requirements. There is no room to assert rights other than as defined in the RFP. If any of the suppliers are unwilling to accept the data requirements and types of license rights outlined, the primes would need to identify and qualify new suppliers willing to accept the government data

right assertions articulated in the OMIT clause. Given the number of vendors who are involved in dual-use technology applicable for both military and civilian applications, this is a very challenging situation. The Air Force's assertion also risks losing some of the most qualified suppliers available in their present zones of expertise. This goes back to the earlier point regarding market priorities—a successful company is not likely to surrender data rights to sell a relatively small run of products when doing so puts significantly larger business opportunities at risk.

The T-X Advanced Pilot Training Program

The T-X Advanced Pilot Training (APT) program was intended to be one of 13 "pathfinder programs" in the ongoing efforts to reduce costs under the Air Force's "Own the Technical Baseline" initiative, which implements DOD's Better Buying Power plan.[36] A planned 350 T-X aircraft are slated to replace the aging T-38C Talon fleet, providing advanced jet pilot training for students preparing to fly fourth, fifth, and future generation fighter aircraft.[37] From an original field of five potential competitors, the contenders have narrowed to a final set of three firms: Boeing/Saab have developed a purpose-designed T-X aircraft as their entry; Lockheed Martin teamed with Korea Aerospace Industries to offer a modernized version of their T-50 jet aircraft; and Leonardo has offered its T-100 jet aircraft, a modification of its existing M-346 trainer.[38]

… a successful company is not likely to surrender data rights to sell a relatively small run of products when doing so puts significantly larger business opportunities at risk.

In order to enable future modernization, the specifications for the T-X require an open system service-oriented architecture. While not requiring full compliance with open mission system (OMS) standards, per the Air Force's RFP language, a company can use OMS standards or proprietary standards to accomplish the goal of building an open systems architecture, but it would have to provide data rights to the US government."[39] OMS, however, did not ameliorate the Air Force's demands for technical and software data rights.

The Air Force included detailed instructions on data rights with the planned T-X acquisition. According to the model contract issued with the RFP, the Air Force has once again defined OMIT to include computer software, declaring OMIT includes: "…all technical data, computer software, computer software documentation, computer data bases and graphics pertaining to the aircraft, ground based training system (academic training, computer based modules, and all types of simulators), and support equipment required to successfully conduct all operation, maintenance, installation, and training activities, regardless of whether such activities are performed by Air Force military, civilian, or contract personnel."[40] Much of the language in the T-X RFP also mirrors that of the UH-1N replacement: data rights flow down to the sub-tier vendors. There does appear to be more wiggle-room in the T-X RFP, allowing vendors with proprietary data to protect that information through assertions, but the CEO letter is still required. Data requirements, and the associated rights, remain a problem for offerings with established supply chains and developed technologies.

Another curve ball exists in this particular competition. The T-X program is slated for a Milestone B entry, with no systems development and demonstration (SDD) phase. Consequently, it brings into question the status of data rights given the necessary investment of the Boeing/SAAB team's new build. Regardless, this is clearly a competition of apples, oranges, and grapes; again, one size cannot fit all. The Air Force should engage in a constructive dialogue with its primes to craft data rights solutions that are unique and fair to each offering; do not impose undue liability on the industry team; satisfy the service's lifecycle needs; and do not artificially favor one vendor over another. A complex issue to be sure, but if the service is willing to entertain complex competitions, it must move past same-and-simple evaluations.

The O/A-X Light Attack Experiment

The Air Force's O/A-X effort is still considered an experiment and is not yet a formal program. Conceived as a way to provide close air support in permissive environments, the effort seeks to relieve high performance combat jet aircraft for employment in more demanding scenarios and help build partnership capacity with

allied nations.[41] According to Secretary of the Air Force Heather Wilson, the O/A-X experiment is a direct response to the National Defense Strategy directing the Air Force to fight violent extremism in a more sustainable fashion, and rely more on allies and partners.

Based on current accounts, consideration is being given to acquisition approaches that might allow for accelerated development and fielding. The O/A-X experiment has thus far been conducted under the other transactional authority (OTA) mechanism that more closely resembles a commercial contract and is structured to encourage collaboration and promote innovation from non-traditional defense contractors. Consideration is also being given to alternate sustainment strategies. Instead of establishing a full 20-30 plus year supply chain to support more traditional weapon system programs, there might be more cost-efficient approaches for a program that might have a shorter life span. Air Force Materiel Command boss Gen. Ellen Pawlikowski noted that the Air Force may "…go to more of a model that accepts that we're going to throw things away after they're not supportable."[42]

Based on current accounts, consideration is being given to acquisition approaches that might allow for accelerated development and fielding. The O/A-X experiment has thus far been conducted under the other transactional authority (OTA) mechanism that more closely resembles a commercial contract and is structured to encourage collaboration and promote innovation from non-traditional defense contractors.

These developments give the O/A-X perfect positioning to pioneer a custom approach to data and software rights. It may be that not only would the O/A-X approach to data and software rights be specific to the uniqueness of the program, but there may also be elements that are tailored to each industry team. Because O/A-X has not yet transitioned to a program of record, there is time for dialogue between the Air Force and private industry teams before the formal solicitation process begins. Similar to the robust discussions that the service is having with companies regarding capability requirements and cost, the Air Force should engage companies to more fully understand industry concerns and articulate Air Force needs.

The Evolved Expendable Launch Vehicle (EELV)

The Evolved Expendable Launch Vehicle space launch program has been ongoing since the 1990s, and is intended to assure Air Force access to space through the use of commercial launch services. There are two EELV related solicitations currently posted to the Federal Business Opportunities (FBO) website. The first of these RFPs call to procure a series of five national security space launches. The second is intended to transition launch services away from reliance on Russian built RD-180 rocket engines to allied rocket engines.

The data rights assertions in both of these solicitations follow the standards outlined in DFARS 252.227-7015, which states that technical data "means recorded information, regardless of the form or method of recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and management information."[43]

Computer software is specifically excluded here from the Air Force's definition of technical data in these solicitations, and therefore complies with DFARS. This is a markedly different model than that employed with the T-X and UH-1N recapitalization programs.

The Ground Based Strategic Deterrent (GBSD)

The GBSD is a program to replace the Minuteman III missile force. The Minuteman missiles comprise the Air Force's intercontinental ballistic missile (ICBM) capability, one of three legs of the US nuclear triad. The program will reuse and update the current ICBM silos and infrastructure but will field an entirely new missile. The Air Force program manager has stressed that the effort has a "…foundation that is a low-risk, mature technology program." At the same time, the manager said that the Air Force intends to employ "…a very detailed own-the-tech baseline strategy and data rights strategy…to make sure we…. get the best value for the government."[44]

According to earlier documents released in the GBSD competition, this will be accomplished by "the government owning key interfaces, specifications, and ensuring government ownership

of technical data" and that the Air Force would employ a "….modular architecture approach which, when coupled with the technical data rights strategy will facilitate a design that will enable future technology insertion, increase competition and improve future sustainability."[45]

While the US government intends to own the technical data for the GBSD program throughout its lifecycle, it did not add an expanded OMIT definition as was done in the aircraft programs, and it adhered closely to existing DFARS clauses in defining software data rights. Specifically, the RFP cited DFARS 262.227-7014, which covers rights in noncommercial software and noncommercial software documentation, which identify restrictions on contractor supplied software with respect to use, release, or disclosure. This DFARS clause also states that, "Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions on the government's rights to use, release, or disclose computer software."

A recent Air Force industry day announcement stated the service's intention is not to acquire significant amounts of contractor off the shelf (COTS) software for the DCGS program…

In 2017, contracts were awarded to two prime contractors, Boeing (for $349 million) and Northrop Grumman ($329 million), for a three-year period of technology maturation and risk reduction. At the end of that period, the Air Force plans to award a single contract to build the GBSD system.

The Open Architecture Distributed Common Ground System

Three years ago, the Air Force began an effort to transition the Distributed Common Ground System (DCGS) to an open architecture. With a legacy extending back to the Contingency Airborne Reconnaissance System (CARS) of the 1990s, DCGS evolved into a global network of ground stations designed to process and exploit surveillance and reconnaissance data from airborne platforms such as the U-2, RQ-4, and MQ-9. Originally developed in a proprietary closed architecture, the DCGS has proven difficult to upgrade in a timely manner. By one estimate, bringing new DCGS capabilities online was taking as long as 84 months, by which time new technologies often made the additions virtually obsolete.[46]

A recent Air Force industry day announcement stated the service's intention is not to acquire significant amounts of contractor off the shelf (COTS) software for the DCGS program, and added the following language to the original data assertions in the first RFI:

> *The contractor shall furnish all technical data, including software, source code, and engineering drawings to enable the government the ability to replicate the software or item. The contractor shall provide all technical data with unlimited rights or justify why it must be provided with less than unlimited.*[47]

This assertion for unlimited rights to manufacturing, process technical data, and the source code of the software exceeds the bounds of the DFARS. The DCGS RFI also offers contractors an opportunity to assert their rights with supporting data for instances in which they believe the unlimited rights assertions may not be appropriate.

However, the Air Force is putting forward this intent during the RFI process; not the final or even draft RFP when industry teams have already assembled their teams, have established supply chains, and have made serious investment in technology. In other words, the timing to make service intent known is much better. Articulating the program's data rights approach early, during the RFI, provides time for companies to develop their technical approach and business strategy around the service's needs. Combined with the fact that this program will not have much commercial content, this is a situation where the Air Force's interests need not diverge dramatically from the offerors. Even so, there is opportunity and time for an industry team to engage in dialogue with the Air Force, and justify a less expansive data rights offering.

Command and Control Systems

Air Force Chief of Staff Gen David Goldfein has identified multi-domain command and control (MDC2) as one his three focus areas. In a "Letter to Airmen" on the subject, Goldfein laid out a vision of a command and control architecture that would support future operations in the air, space,

and cyber domains and do so with a command and control system that would incorporate "…common architectures, standardized data formatting, increased machine-to-machine and artificial learning systems, and better integration…"[48]

Transitioning to the future vision of MDC2 requires a fundamentally new approach and underlying concepts: doctrine is still being developed. Of the acquisition programs described in this paper, MDC2 is the farthest-leaning into the future. Functionally, MDC2 is intended to feature three key attributes: "… extremely high quality situational awareness, rapid decision making, and the ability to direct forces across domains and missions with continuous feedback."[49] In technological terms, this implies architecture capable of incorporating rapid changes and upgrades in order to pace the threat and evolving operational requirements.

The Air Force should not wait to announce its intention on data rights. While it is prudent to assume that the bulk of the fielded MDC2 technologies will be developed in a traditional manner of down-select and SDD, it is also fair to conjecture that the seeds of this advanced technology may currently exist primarily in commercial companies.

The Air Force has not published a new solicitation related to the MDC2 effort, but the search for new technologies has formally begun. In December 2017, the Air Force Research Labs published an RFI under the title of "Mastering Complexity in Multi Domain Command and Control." This RFI cites three key technology areas. Complex adaptive systems address the rapidly expanding complexity of multi-domain command and control in future combat, shifting systems from linear to non-linear architectures. Complex effects analysis develops operational effects in a multi-domain environment. Finally, machine intelligence improves system characterization of the operational environment and augments human decision makers.[50]

This RFI does not address the data and software rights with respect to the eventual RFP, though it should. The Air Force should not wait to announce its intention on data rights. While it is prudent to assume that the bulk of the fielded MDC2 technologies will be developed in a traditional manner of down-select and SDD, it is also fair to conjecture that the seeds of this advanced technology may currently exist primarily in commercial companies. This may be a program where the pace of commercial innovation on cognitive computing, machine learning, and neural networks has outpaced the DOD, and those commercial technologies will set the foundation for military capabilities. MDC2 will require up-front analysis of its inherently complex data rights by the government with strong involvement with industry. If the eventual RFP surprises with overreach as in the UH-1 or T-X solicitation, this critical acquisition can expect problems from protest, less competition, less innovation, and schedule delays.

Points for Discussion

The Air Force's Inconsistent Approach to Data Requirements and Rights

Wholly proprietary systems are not in the interest of the Air Force, and therefore not in the interest of any defense industry prime or team. But neither is the overreach demonstrated in recent competitions.

Most all involved in acquisitions fundamentally understand the operating environment far better and what it means to build, maintain, and sustain an information age force. Increased use of commercial subsystems; proprietary IP across small businesses and large commercial companies; unprecedented service life of weapons systems; the speed of technological advancements, and the need to modernize and sustain in a cost-effective manner are all features that complicate the landscape for requirements and rights. While the US government's intention to protect its interests are understandable, it needs to do so in a fashion that aligns with the broader interests of both the traditional defense and the commercial marketplace. The Air Force's position appears to be evolving, yet it remains unclear whether the service fully understands how their actions are shaping and incentivizing industry behavior: near-term wins on programs may result in long-term industrial base losses for everyone involved. Given the information reviewed in this paper and seen elsewhere, it is not clear that the Air Force has a consistent approach to data rights and data requirements.

Both the UH-1N and the T-X RFPs feature language that expanded the definition of OMIT data to include computer software. This inclusion of computer software in the definition of OMIT, which would confer unlimited rights to the government, is disputed by experts in the field. The leading industry association representing aerospace firms has asserted that this language, in the context of the recently canceled JSTARS replacement RFP, "…extends the unlimited rights OMIT concepts to 'Computer Software' as defined in DFARS 252.227-10141014, all of which is neither technical data nor subject to OMIT/unlimited rights. As such, it is arguably in violation of 10 U.S.C. 2320(a)(2)(F) in that it requires a contractor to give rights in software available under DFARS 252.227-7014."[51] This analysis similarly applies to how software has been defined in the UH-1N RFP.

MDC2 is likely to have more complicating factors, given the probability that much of the technical foundation may originate in the commercial realm. The program also appears late to open an explicit dialogue with industry on what may become a contentious issue.

Whereas the expanded OMIT definition in the case of the UH-1N made no provision for bidders to assert protection for proprietary software, the T-X RFP did, in fact, include language permitting bidders to protect proprietary software.

The GBSD program would appear to be more complex than either the UH-1N replacement or the T-X, and will have a life span extending over multiple decades. Given that, it is unclear why the Air Force is pursuing a more expansive and intrusive approach to data rights in these aircraft programs, while opting for more traditional data rights approaches in the case of GBSD, which is arguably a much more complex program. The answer may be that the GBSD program office is simply following precedent and standard in their directorate. After all, the EELV program also employs a more traditional data rights approach; neither program asserts more expansive data rights clauses than seen in the past.

The Air Force intends to assert broad, unlimited technical and software rights in open architecture DCGS. Because the service intends to have very little commercial content and intends to federally fund software development, it appears that the Air Force's approach may not impose the same disincentives or financial liabilities on defense primes the previous examples exposed. Perhaps most important is the timing of the Air Force's assertion, and their openness to dialogue with industry. In other words, this is a case where data rights could be tailored to meet the context of the program, the needs of the Air Force, and the interests of industry.

Unfortunately, MDC2 is likely to have more complicating factors, given the probability that much of the technical foundation may originate in the commercial realm. The program also appears late to open an explicit dialogue with industry on what may become a contentious issue. Because the acquisition team has not announced their approach, MDC2 has the potential to follow a similar path of dialogue to craft a deliberately tailored approach; but they should do it sooner than later.

Data rights, as defined today, are actually a fairly straight-forward topology. While OMIT lacks an explicit definition, there is precedent for a codified understanding of what constitutes OMIT, and the DFARS are clear on what is not included in technical data and software. Technical data and software can then be identified as commercial and non-commercial. Finally, when overlaid by source funding—that is, who invested in the development of the technology or software—content and scope of data rights becomes much clearer. The challenge faced by both the DOD and industry is that the Better Buying Power initiatives are blurring the lines between traditional defense and commercial. Leveraging the affordability of commercial items and software into defense hardware and systems complicates the US government's understandable desire to expand their data rights ownership. The movement by DOD to push traditional defense primes to make non-reimbursable investments into technology development means that the concerns of intellectual property and the technical data and software rights that protect that IP no longer just apply to commercial companies.[52] Finally, the environment has also changed, and in a way that sets the DOD and the defense and commercial industry at odds. The increased value of software and technology to weapons system capabilities make it increasingly important for the US military to acquire liberal licensing—just as that same

value has increased the imperative for companies to more strongly assert their data rights to preserve their IP.

The DOD's Better Buyer Power 3.0 advocates for removing barriers to commercial technology use in defense programs to reduce costs and attract more innovation. But it does not appear that the government truly understands the complexity of defense and commercial industry business models and incentives, or even more importantly, how their new policies will shape industry behavior over the long term. For example, highly innovative companies that appropriately value their IP may be disadvantaged by acquisition processes. The Defense Business Board went so far as to suggest that the current acquisition system was more likely to be "…fair to the non-innovator, low-value player who has mastered the bid and proposal system." [53] Companies know how to play the proposal evaluation game, and they play to win. As a result, they may not invest in or offer leading-edge technologies because to do so could make them uncompetitive; alternately, underbidding would dilute their company's value. Any company must maintain competitive advantage in the market place and, especially in technology driven businesses, that means innovating and earning a return on the intellectual property (IP) developed for a given market. The licensing of the IP associated with innovative technology comes with the expectation of profitability and profitability is tightly linked to a company's ability to acquire capital to continue to innovate. When that ability is eroded, a given market becomes less attractive and, potentially for some, untenable.

…even if the DOD were to attempt to compensate companies for their data rights, either outright or through the Value Added Total Evaluated Price (VATEP) evaluation of a proposal, the government does not appear to have an effective process for conducting IP valuation.

An additional problem that must be grappled with is that even if the DOD were to attempt to compensate companies for their data rights, either outright or through the Value Added Total Evaluated Price (VATEP) evaluation of a proposal, the government does not appear to have an effective process for conducting IP valuation.[54] What is IP and its associated data rights worth? Government acquisition officials are just not well versed in the subject, and understandably so. Because of the nature of historical defense technology development, IP valuation has not been an issue the DOD has had to manage. It is the DOD's movement to increasing commercial technologies and content as well as shifting R&D investments to industry that is complicating of data rights. The difficulty in developing a common understanding between government and industry with respect to IP valuation (and therefore technical and software data rights) represents an obstacle to arriving at a common understanding of the role of IP and data rights in propelling innovation and in maintaining a healthy defense industrial/innovation base.

Understanding Innovation Models

Innovation comes in many forms, but two forms are particularly relevant to this discussion. The first of these is continuous evolutionary technology development. A weapon system is built, and continually improved. The C-130 has been in the Air Force inventory since the 1950s and, in its latest configuration, the C-130J, continues to be a mainstay in the US tactical airlift fleet. The B-52, originally developed as a nuclear bomber in the 1950s, may now be in service for close to a century with planned modifications and engine upgrades. These systems represent continuous evolutionary innovation based on established IP. It is this iterative, long-term sustainment and modernization and innovation challenge where the DOD understandably seeks to avoid vendor lock. The challenge for DOD, and industry, on this evolutionary, iterative innovation model is to appropriately value and reward the OEM for their initial development and incentivize the OEM's continued innovation while owning the necessary and sufficient type and level of technical and software data rights to facilitate the long-term sustainment and modernization of the system in a way that is not beholden to the OEM.

The flip side of evolution is the discontinuous, game-changing innovation that preserves our qualitative military superiority well into the future. Some of this disruptive innovation may come from within the defense establishment, but much of it will be based on technologies developed for non-defense purposes. Yet, the rapidly innovating commercial technology sector in our economy

does not need government work in order to be financially successful. These companies will not be putting their commercial revenue at risk in order to compete on government contracts. One mid-sized aerospace company interviewed for this project indicated they would likely forego government work in order to preserve their commercial work, if forced to make a choice to protect their intellectual property. Such companies may perceive government data rights assertions as overly aggressive, and that places their IP at risk in ways that could harm their primary businesses.

Firms are increasingly harnessing dual-use technologies to deliver value, capability, and speed the acquisition process at lower cost, while still procuring high quality products from innovative commercial suppliers. This is exactly the type of scenario where a precise data rights policy is required, not a blanket approach that may put vendors who have significant interests in the civilian and traditional defense marketplace at risk. It would be one thing if the government unilaterally funded the development of these dual-use systems, but they do not. Demanding the intellectual property for something developed with private funding for dual-use applications lacks foresight, and may preclude many vendors from wanting to participate in government acquisition programs.

Firms are increasingly harnessing dual-use technologies to deliver value, capability, and speed the acquisition process at lower cost, while still procuring high quality products from innovative commercial suppliers. This is exactly the type of scenario where a precise data rights policy is required…

The challenge facing the DOD is not an easy one. For the Air Force, technical and software data rights are a particularly important issue. The Air Force is perhaps the most technologically-oriented of all the services, and it is balancing the demands of recapitalizing in a way that will be relevant for decades to come while concurrently sustaining and modernizing an aged fleet. This means that the Air Force must preserve programmatic initiative and flexibility for future competition, and do so in a way that properly rewards, incentivizes, and cultivates its industrial base. However, budget pressures are not going away, and cost is a driver in every decision. The Air Force must have sufficient data with associated rights to support a lifecycle of competition that drives cost down and brings the best technology forward for modernization. But the service should be cautious to not overreach; to do so risks actually increasing program lifecycle costs, exiting or consolidating small business suppliers, reducing overall competition, and constraining participation from innovative vendors and non-traditional companies.

Finding the Right Balance: Recommendations for Action

As the DOD continues to transition military force structure and capabilities into the information age, technical data and software rights issues will increase in importance. Just as each program will have different capability and performance requirements, each will also have different sustainment and modernization needs across their lifecycle. No acquisition is the same, and data requirements and rights should not be treated the same across those acquisitions. It is up to the Air Force to ensure that they articulate their technical and software data requirements and data rights intentions early, so that industry can be responsive in their offer. Prime contractors will be sensitive to the RFP and the evaluation methodology; industry will assemble a team of partners and suppliers to provide what they believe will be the most competitive proposal. It is up to the Air Force to fully understand how their actions, RFPs, and evaluations incentivize and shape industry behavior—and as a consequence, the force structure and capabilities of the Air Force.

This is truly a case where government and industry all win together, or all lose together. A data requirements and rights acquisition strategy must be a fundamental part of any solicitation. The Air Force should be alert to the possibility that asserting data rights beyond the accepted definitions in the DFARS, or that demanding data rights concessions beyond those required by statute, may have unintended negative consequences downstream that inhibit, rather than encourage, defense innovation. Early and iterative discussions with industry during the RFI process can help the Air Force more fully understand their near- and long-term data rights requirements. Doing so will ensure that when the service crafts their final RFP,

they have considered the potential consequences of various data rights strategies and have selected a deliberate and tailored approach that achieves the best outcomes for all.

To that end, the following recommendations are offered for consideration.

1. Develop a Series of Data Rights "Templates" that Flexibly Adapt to Program Needs: No program is the same, and therefore no data right acquisition strategy will be the same. However, there will be sufficient similarities between types of acquisitions that having baseline templates would prove useful to acquisition teams. Data requirements and rights can be nuanced and esoteric, and it is not always realistic to expect that each acquisition officer be an expert in the subject. These tools should guide teams through the process of determining which template would be appropriate to that particular program, and how to adapt that template to the specifics of the acquisition. The templates should have sufficient granularity to provide actual value to the program acquisition officers who may struggle to define the specific licensing necessary to support the lifecycle needs.

To achieve effective data acquisition strategies, it is critical to improve the acquisition corps' level of understanding of industry incentives, business models, and IP valuation.

It is important that this initiative avoid the pitfalls described earlier in this paper regarding the unintended consequences of overly aggressive or unilateral data rights assertions by either party. To that end, a team of Air Force acquisition and industry professionals should partner to develop the templates and associated guidance materials that will assist acquisition teams in understanding and crafting their IP approach. Partnering together will invest industry in the outcome and gain greater buy-in; facilitate a more predictable and deliberate service approach to industrial base IP concerns; and develop more creative and effective solutions achieve the long-term needs of the Air Force.

2. Stand Up a Cadre of Acquisition Officers that Specialize in Data Rights: US government personnel working in acquisition and contracting seldom have actual industry experience. To achieve effective data acquisition strategies, it is critical to improve the acquisition corps' level of understanding of industry incentives, business models, and IP valuation. It is unrealistic, however, to simply levy additional training requirements onto an already stressed and undermanned career field, especially for a subject that is so complex. Instead, the Air Force should hand-select and train a cadre of acquisition professionals who specialize in data requirements and licensing. This group would act as on-call specialists for the broader acquisition corps. They would provide expertise at any point in a program's lifecycle, from the development of data requirements and the types of licensing needed to the evaluation of submitted proposals and annual contract negotiations or other sustainment and modernization issues.

These specialists would also cultivate and sustain strong relationships with Industry, almost acting like an ombudsman for industrial data rights concerns. They should have the ability to impartially understand the concerns of industry and help both sides come to an appropriate resolution. This team would partner with both traditional and commercial industry to understand best practices and develop a common method of IP valuation to be used for evaluation within government solicitations, and fairly adjudicate corporate data rights concerns, such as undervaluing the IP and the associated data rights. This would include budgeting for any commercially unusual IP or data rights, and the ability to monetize various courses of action when it comes to content and scope of data rights. This data rights cadre must have a strong command of the impact of government data requirements and rights on the broader health of a franchise, company, innovation investments, and the larger industrial base; as well as objectively assess the long-term needs of the Air Force.

3. Develop a Standardized, Rigorous, Enforced Process for Determining Data Requirements and Rights: A major finding of this paper is that there does not appear to be an enforced process for putting analytical rigor behind what data and what kinds of rights the Air Force will need for the lifecycle of a given program. The Air Force should develop a data requirements process that mirrors (and is closely tied to) capability requirements development, the sustainment strategy, and modernization planning. Informed by industry best practices and adapted to the needs of the government, this process would

provide rigor to a data rights/cost curve similar to that used to optimize capability requirements This process is not expected to result in a "one size fits all" approach that indiscriminately sweeps up data or takes a cut-and-paste approach; rather, it should acknowledge that each program is unique and will have specialized needs. A well-understood process will help industry provide an offer that can support long-term Air Force requirements. Data requirements and rights are so important to both the government and the industrial/commercial base that they cannot be handled in an ad hoc or knee-jerk manner. The Air Force must provide structure to better understand immediate and future licensing needs, incorporate industry dialogue early in the RFP development process, and facilitate a better understanding of near- and long-term data rights cost.

Proposed data requirements and rights should be a topic for discussion in the development of any major solicitation, just as capability and performance requirements are.

4. Government-Industry Discussions: Data requirements and rights must be right-sized: the US government should engage in discussions with industry early in the acquisition process to determine the best scope of technical and software data rights across the program lifecycle, and the potential consequences of various approaches under consideration. Proposed data requirements and rights should be a topic for discussion in the development of any major solicitation, just as capability and performance requirements are. When coupled with tailorable templates, support from the data rights cadre, and informed by RFIs, industry days, and engagement and dialogue, this process should proactively receive and shape industry response towards a final RFP that best meets Air Force needs. The Air Force must better understand potential benefits and ramifications of different approaches to data rights and requirements. This would permit better mutual understanding of potential ramifications of differing approaches to data and would permit industry to articulate the potential costs that ensure from differing approaches to licensing rights.

5. Include the Data Requirements and Rights in Standard Acquisition Strategy Reviews: An effective and appropriate data requirements and rights process should be evidenced by an IP strategy that is more refined in new solicitations, and ensures the data requirements match identified needs that are well defined and understood. As each program acquisition strategy progresses through the various reviews, special consideration should be made to avoid contracting for excess or unnecessary IP while simultaneously cross-pollinating for best practices and emerging issues. These reviews, conducted concurrently with the standard acquisition strategy reviews, should ensure that the data requirements and rights strategy complies with both the letter and the spirit of statute, regulation, and precedent. This would include walking back any "creep" that has occurred in recent acquisitions.

Specifically, the inclusion of software code in the definition of OMIT appears to conflict with the applicable statues and precedent. Software source code should not be included in OMIT since the concept of OMIT for hardware relates to returning the hardware to its original condition, whereas changes to source code to correct deficiencies necessarily results in a different software program. This is not to say that software code should be excluded completely from any data rights package sought by the government; rather, it is to assert the unique nature and value of software code to the vendor and to acknowledge that the Air Force's need for software code must be addressed through means other than OMIT.

6. Utilization of Specially Negotiated Licenses (SNLs): While new DOD guidance requires the negotiation of data rights pricing in all major weapon system solicitations, it does not entitle the government to the acquisition of unlimited rights at expanded levels or that such acquisition would be free. Any strategy should fairly value the IP sought, and through a more refined technical data rights strategy. The tailored approach advocated for in previous recommendations would be well supported through the use of Specially Negotiated Licenses (SNLs). SNLs also offer a promising approach to resolving the contentious issues surrounding software code. Finally, SNLs provide the Air Force a venue to match non-standard sustainment and modernization timelines to the data rights granted through licensing. Not all data is needed at once, or even at the same Milestone. The government must

improve its planning process to account for the data and licensing required to be delivered immediately versus what is needed for later sustainment and modernization. Such targeted licensing prevents the government from unnecessarily inflating the cost of a license or program, and limits the IP and financial exposure of a company. This is what the current laws and regulations require, and is also the main thrust of the proposed changes coming out of the "813 Panel." By improving the planning process early in the acquisition and utilizing SNLs that can meet unique needs, the problems induced by a broad and indiscriminate data approach can be avoided while ensuring the government's needs are met.

7. Commercial Products: When commercial products are modified to meet DOD requirements, they should continue to be treated as commercial products with regard to pricing and data rights, even when those products are part of a supply chain or sub-tier vendor. This recommendation is in line with the intent of cost-efficiency initiatives by the DOD and Better Buying Power 3.0. The government should procure such items under FAR Part 12 Acquisition of Commercial Items and not Part 15 Contracting by Negotiation. The government should not attempt to obtain commercially unusual IP or data rights to such products or to their DOD funded modifications. This is also a conclusion of the "809 Panel" established under Section 809 of the National Defense Authorization Act for Fiscal Year 2016.

When commercial products are modified to meet DOD requirements, they should continue to be treated as commercial products with regard to pricing and data rights, even when those products are part of a supply chain or sub-tier vendor.

8. Review the Expiration Timelines of Government Purpose Rights: Technology suppliers in the government market often operate in both government and commercial markets, yet their IP may be better protected for longer periods of time in the commercial sector. For many small, innovative companies of the type the government wants to attract, these disparities between the commercial sector and government protection of IP represent a disincentive to participate in government programs. Moore's Law, which stipulates the steady increase of microchip processing power over time, does not compress proprietary IP timelines or render them obsolescent. Instead, the increasing speed of technological development makes protecting data critical to providing a sound foundation that encourages a diversity of innovation. In order to facilitate strong and cost effective commercial options, the government should match the natural cycle of the commercial market and consider longer durations for treating IP as proprietary. The acquisition cadre should work with industry to review the timelines of commercial standard practices for IP protection to determine whether the current five-year protection under government purpose rights should be revised to better align with commercial technology markets.

9. The 813 Panel: Like the 809 Panel before it, the 813 Panel was established under Section 813 of the Fiscal Year 2016 National Defense Authorization Act. The purpose of the 813 Panel is to review Title 10 US Code 2320 and 2321 regarding technical data rights and the validation of proprietary data restrictions. Specifically, the 813 Panel is charged with providing data rights recommendations that encourage private sector investment and innovation, appropriate reward and value industry IP, and facilitate the long-term sustainment and modernization needs of the services. As of this writing, the work of the 813 Panel remains in draft. However, based on the information thus far available, it appears that the recommendations contained in this paper are consistent with the general thrust of the 813 Panel's conclusions and recommendations.

Conclusion

The ability of the United States Air Force to prevail in the challenging environment of 21st Century multi-domain warfare is inextricably linked to the technological superiority of the weapon systems the Air Force procures and operates. In order to successfully operate, sustain, and modernize those weapons systems in a rapid fashion that yields the best capabilities, the Air Force needs access to more data than it has had in the past. Today's weapons systems are more heavily software dependent, but the service has not yet adapted its acquisition policies to address data requirements. The acquisition process that serves the Air Force today was developed for the

last century's hardware-centric force, and simply is not quite up to the task of identifying what data and what types of licenses the service will need over the span of a weapons system's lifetime.

While the government clearly has growing needs for procuring and using data, it also has a responsibility to meet those needs in ways that encourage private investment and competition. Achieving these goals requires a mutually beneficial relationship between the Air Force and the defense industrial base. This relationship depends on both the continued competitiveness of traditional prime contractors, their suppliers, and the ability to attract new commercial technology innovators into support the Air Force. Industry must also remain competitive to secure future work with the Air Force. However, the Air Force is also in competition—with commercial markets—to attract cutting edge technology to the defense market. When the government overreaches with IP and data rights, it abrogates this responsibility by asking for data it does not need, or for licenses well in excess of any possible use for this data. The result of such an expansive approach is the government may have the ability to call on fewer contractors (especially at the subcontractor and small business level), leading to a reduction in competition, and discouraging meaningful non-federal investment.

The factors driving the Department of Defense and the Air Force to seek greater access to data are rational and reasonable, as are the marketplace dynamics that make protecting intellectual property an imperative for industry. Both the Air Force and Industry must share an understanding of the critical role that intellectual property plays in the ability of defense suppliers to develop and maintain future technological superiority, and what access the Air Force requires to sustain and modernize their weapons systems for the decades to come. The answer cannot be all or nothing. To build and maintain a 21st century Air Force that the United States requires, the service must work with industry to create a modern acquisition environment that sets the conditions for mutual success in the future. ✪

Endnotes

1 "Mitchell Hour – Air Force Lt Gen Lee K. Levy," YouTube recording of Mitchell Institute presentation, comments at 10:15, posted by Mitchell Institute, May 23, 2018, https://www.youtube.com/watch?v=A70dlkoqpbQ (all links accessed June, 2018).

2 Department of Defense, *DFARS Subpart 227.71 – Rights in Technical Data*, Section 227.7103 (Washington, DC: DOD), https://www.acq.osd.mil/dpap/dars/dfars/html/current/227_71.htm.

3 US Air Force, Office of the Staff Judge Advocate, Space and Missile Systems Center (SMC), *Acquiring and Enforcing the Government's Rights in Technical Data and Computer Software Under Department of Defense Contracts* (Fort Belvoir, VA: Defense Acquisition University, May 2017), https://www.dau.mil/tools/t/TDR-GB.

4 Cornell Law School, Legal Information Institute, Rights in Technical Data, 10 USC 2320(a)(2)(C)(iii) (December 2017), https://www.law.cornell.edu/uscode/text/10/2320.

5 Government-Industry Advisory Panel, *Section 813 Panel Tension Point Paper: Are Existing Rights Sufficient for Maintenance and Sustainment?* (February 2018), draft. Authors' note: This draft point paper is part of the advisory panel's work regarding maintenance and sustainment practices and data rights, and can be accessed by registering with the Federal Advisory Committee Act (FACA) database, which can be found here: http://facadatabase.gov.

6 "Data Rights," Defense Information Systems Agency, accessed June 2018, https://disa.mil/About/Legal-and-Regulatory/DataRights-IP/DataRights#1.

7 Ibid.

8 Ibid.

9 Ibid. Authors' note: Also see DFARS Section 227.7103.

10 Defense Information Systems Agency, "Data Rights: What License Rights does the Government Obtain in Technical Data and Computer Software Developed Under a Government Contract?" https://disa.mil/About/Legal-and-Regulatory/DataRights-IP/DataRights#1.

11 Frank Kendall, "Implementation Directive for Better Buying Power 3.0—Achieving Dominant Capabilities through Technical Excellence and Innovation" (official memorandum, Washington, D.C.: Department of Defense, April 2015) https://www.acq.osd.mil/fo/docs/betterBuyingPower3.0(9Apr15).pdf, 9.

12 Mitchell Institute for Aerospace Studies, "Mitchell Hour – Air Force Lt Gen Lee K. Levy," May 23, 2018

13 Authors' note: For additional information see 10 USC 2320(e). The intellectual property strategy is required under DOD Instruction 5000.02

14 Jack L. Brock, *Intellectual Property: Industry and Agency Concerns Over Intellectual Property Rights*, GAO-02-723T (Washington, D.C.: Government Accountability Office, 2002), https://www.gao.gov/new.items/d02723t.pdf.

15 William M. Solis, *DOD Should Strengthen Policies for Assessing Technical Data Needs to Support Weapon Systems*, GAO-06-839 (Washington, D.C.: GAO, July 2006), www.gao.gov/cgi-bin/getrpt?GAO-06-839.

16 William T. Woods, *Government Contracting: Early Attention in the Acquisition Process Needed to Enhance Competition*, GAO-14-395 (Washington, D.C.: GAO, May 2014), https://www.gao.gov/assets/680/678888.pdf.

17 Cornell Law School, Legal Information Institute, Negotiation of Price for Technical Data Before Development or Production of Major Weapon Systems, 10 US Code § 2439 (December, 2017), https://www.law.cornell.edu/uscode/text/10/2439.

18 Weapon Systems Acquisition Reform Act of 2009, Pub. L. No. 111-23, 123 Stat. 1704 (200). https://www.acq.osd.mil/parca/docs/2009-05-22-pl-111-23.pdf.

19 Defense Logistics Agency, *Department of Defense Standard Practice Technical Data Packages*, MIL-STD 31000 (Washington, D.C.: DLA, December 2017), http://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=276980.

20 National Defense Authorization Act for Fiscal Year 2017, Conference Report to Accompany S. 2943, 114th Cong., Second Session, Report 114-840 (November 30, 2016), https://www.acq.osd.mil/dpap/dars/docs/FY_2017_NDAA.pdf, 12.

21 Daniel Chudd, Catherine Chapple, and Locke Bell, "What Contractors Need to Know About the Proposed FY 2018 NDAA," Morrison & Foerster's *Government Contract Insights,* November 16, 2017, http://govcon.mofo.com/defense/what-contractors-need-to-know-about-the-proposed-fy-2018-ndaa/.

22 Dr. William LaPlante, former Assistant Secretary of the Air Force for Acquisition, author interview, May 10, 2018.

23 Defense Innovation Board, "Ten Commandments of Software"(working document, draft version 0.14, last modified April 15, 2018), https://media.defense.gov/2018/Apr/22/2001906836/-1/-1/0/DEFENSEINNOVATIONBOARD_TEN_COMMANDMENTS_OF_SOFTWARE_2018.04.20.PDF.

24 Sandra Erwin, "Pentagon Advisory Panel: DoD Could Take a Page from Space-X on Software Development," *Space News*, April 10, 2018, http://spacenews.com/pentagon-advisory-panel-dod-could-take-a-page-from-spacex-on-software-development/.

25 W.J. DeVecchio, "Feature Comment: Data Rights Assault: What in the H (Clause) Is Going On Here? Air Force Overreaching on OMIT," *The Government Contractor*, Vol. 60, No. 2, January 17, 2018, https://media2.mofo.com/documents/180117-air-force-omit-data.pdf.

26 Ibid.

27 LaPlante, author interview, May 10, 2018.

28 Authors' note: BBP 3.0 is the next iteration of DOD's Better Buying Power and includes the following tenets: "Achieve affordable programs…Achieve dominant capabilities…While controlling life cycle costs…Incentivize productivity in industry and government…Incentivize innovation in industry and government…Eliminate unproductive processes and bureaucracy…Promote effective competition…Improve tradecraft in the acquisition of services…Improve the professionalism of the total acquisition workforce…Improve the professionalism of the total acquisition workforce." For a more complete discussion, read the complete BBP 3.0 paper at: http://bbp.dau.mil/docs/BBP3.0FactSheetFINAL.pdf.

29 Frank Kendall, "Implementation Directive for Better Buying Power 3.0—Achieving Dominant Capabilities through Technical Excellence and Innovation," https://www.acq.osd.mil/fo/docs/betterBuyingPower3.0(9Apr15).pdf, 2.

30 LaPlante, "Owning the Technical Baseline – A Key Enabler," *Defense AT&L* (July-August 2015), dau.dodlive.mil/files/2015/06/LaPlante.pdf.

31 Defense Acquisition University's ACQuiPedia, "Technical Baselines," accessed June 12, 2018, https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=1029714a-8dcb-43c3-9d2c-30434709d4f0.

32 Jared Serbu, "DOD Brings Culture of Open Architecture to a World of Proprietary Systems," Federal News Radio, November 13, 2013, https://federalnewsradio.com/defense/2013/11/dod-brings-culture-of-open-architecture-to-a-world-of-proprietary-systems/.

33 Authors' note: Similar OMIT clauses were also included within the Air Force's KC-46 and E-8 JSTARS programs; those programs are not addressed in this discussion because the KC-46 is already well underway and the JSTARS program is under revision.

34 Valerie Insinna, "Lockheed Filed a Pre-Award Protest of the Air Force's Huey Replacement Competition. Here's Why," *Defense News*, February 20, 2018, https://www.defensenews.com/air/2018/02/20/lockheed-filed-a-pre-award-protest-of-the-air-forces-huey-replacement-competition-heres-why/.

35 Air Force Life Cycle Management Center, *UH-1N Replacement Air Vehicle Request For Proposals* (Wright-Patterson AFB, Ohio: July 13 2017), https://www.fbo.gov/utils/view?id=38d4fdbf62ac42f7ee0c434b43879544.

36 LaPlante, "Owning the Technical Baseline – A Key Enabler," *Defense AT&L*.

37 Charlsy Panzino, "Joint Base San Antonio-Randolph Will Be First To Get New T-X Trainer," *Air Force Times*, February 22, 2018, https://www.airforcetimes.com/news/your-air-force/2018/02/22/joint-base-san-antonio-randolph-will-be-first-to-get-new-t-x-trainer/.

38 Oriana Pawlyk, "Air Force Delays Contract for T-X Replacement Until Spring," *Military.com*, October 17, 2017, https://www.military.com/dodbuzz/2017/10/17/air-force-delays-t-x-contract.

39 US Air Force Materiel Command, *T-X Request For Proposals FA8617-17-R-6219*, Model Contract, Part I- Section H – Special Contract Requirements, p 65.

40 Ibid.

41 Bryan Ripple, "Light Attack Experiment: A New Way of Doing Business for the Air Force," 88th Air Base Wing Public Affairs, Wright-Patterson AFB, Ohio, August 18, 2017, http://www.wpafb.af.mil/News/Article-Display/Article/1282308/light-attack-experiment-a-new-way-of-doing-business-for-the-air-force/.

42 John Tirpak and Brian Everstine, "Pawlikowski Says Throwaway Tech May Help Speed Fielding; May Affect OA-X," *Air Force Magazine*, March 14, 2018, http://www.airforcemag.com/Features/Pages/2018/March%202018/Pawlikowski-Says-Throwaway-Tech-May-Help-Speed-Fielding-May-Affect-OA-X.aspx.

43 Air Force Space Command, US Air Force Space and Missile Systems Center, *EELV Phase 1A Request for Proposal 1A-6,* (Los Angeles AFB, CA: Added November 6, 2017), https://www.fbo.gov/index?s=opportunity&mode=-form&id=cc4fe6a113403f3a7b1d79cee4a123ff&tab=core&_cview=1

44 Wilson Brissett, "Replacing Minuteman," *Air Force Magazine.* February 2018, http://www.airforcemag.com/MagazineArchive/Pages/2018/February%202018/Replacing-Minuteman.aspx.

45 Air Materiel Command, *Ground Based Strategic Deterrent RFI,* FA8219-15-R-GBSD-RFI1 (Wright-Patterson AFB, OH: January 23, 2015), https://www.fbo.gov/index?s=opportunity&mode=form&id=64f0781d91f486ab27724cc75ad-95cb0&tab=core&_cview=1.

46 M. Wes Haga, "How the US Air Force Made Its ISR Network Cheaper to Run and Easier to Upgrade," *Defense One*, October 16, 2017, https://www.defenseone.com/ideas/2017/10/how-us-air-force-made-its-isr-network-cheaper-run-and-easier-upgrade/141806/

47 Air Materiel Command, Air Force *DCGS Agile Requirements Multiple Award/Indefinite Delivery/Indefinite Quantity Draft Statement of Work*, FA8730-18-R-0009 (Wright-Patterson AFB, OH: April 13, 2018), https://www.fbo.gov/index.php?s=opportunity&mode=form&id=51a5d6495631fb2c9d6e6db6b3da-be7e&tab=core&_cview=0.

48 Gen David Goldfein, "Enhancing Multi-Domain Command and Control… Tying it All Together" (CSAF Letter to Airmen, Washington, D.C.: Office of the Chief of Staff, US Air Force, March 10, 2017), http://www.af.mil/Portals/1/documents/csaf/letter3/Enhancing_Multi-domain_CommandControl.pdf.

49 Daniel Goure, "The Next Revolution In Military Affairs: Multi-Domain Command and Control," *Real Clear Defense*, December 6, 2017, https://www.realcleardefense.com/articles/2017/12/06/the_next_revolution_in_military_affairs_multi-domain_command_and_control_112741.html.

50 Air Force Research Laboratory, *Mastering Complexity in Multi Domain Command & Control (MDC2)*, RFI-AFRL-RIK-18-02 (Rome, NY: December 20, 2017), https://www.fbo.gov/index?s=opportunity&mode=form&id=5a8ce4f-587e5855cd33cf7ba14422a41&tab=core&_cview=1.

51 Aerospace Industries Association, *Aerospace Industries Association (AIA) Response to Government-Industry Advisory Panel's Request for Information on Rights in Technical Data and the Validation of Proprietary Data Restrictions*, 81 Fed. Reg. pp. 40290-92 (Arlington, VA: AIA, August 15, 2016). Author's note: Because the Air Force announced its intent to cancel the program, the JSTARS recapitalization was omitted from this paper's analysis. However, because the JSTARS recap RFP also followed similar trends in computer software, OMIT definition, and data rights, analysis of that RFP remains relevant to this work.

52 Scott Maucione, "New DOD Research Policy Gets Glowers from Industry," Federal News Radio, November 8, 2016, https://federalnewsradio.com/defense-industry/2016/11/dod-makes-changes-research-policy-ticks-off-industry/.

53 Defense Business Board, *Report to the Secretary of Defense, Innovation: Attracting and Retaining the Best of the Private Sector* (Washington, D.C.: DSB, June 2014) http://dbb.defense.gov/Portals/35/Documents/Reports/2014/DBB-FY14-02-Innovation%20report%20(final).pdf.

54 Author's note: According to DAU: "Value Adjusted Total Evaluated Price (VATEP) is a tradeoff source selection process where the offeror's total proposed price may be adjusted based on the "value" placed on better performance as identified in the solicitation. The Source Selection Authority (SSA) must then determine if a higher rated technical offer is "worth" the additional cost to the Government." For more information, see DAU's acquisition encyclopedia resource on VATEP: https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=fe872ab3-5898-4aa5-b6b9-c00a409f633d.

About The Mitchell Institute

The Mitchell Institute educates about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Series

The Mitchell Institute Policy Papers is a series of occasional papers presenting new thinking and policy proposals to respond to the emerging security and aerospace power challenges of the 21st century. These papers are written for lawmakers and their staffs, policy professionals, business and industry, academics, journalists, and the informed public. The series aims to provide in-depth policy insights and perspectives based on the experiences of the authors, along with studious supporting research.

About the Authors

Col Herbert C. Kemp, USAF (Ret.), PhD, served 28 years as an Air Force intelligence officer. His assignments included command, staff, and diplomatic tours, serving in Asia, the Middle East, Europe, and Latin America. In his final active duty assignment prior to his retirement in 2001, Kemp served as deputy director for surveillance and reconnaissance, Headquarters Air Force, Pentagon, Washington, D.C. He is currently the president and CEO of OneALPHA Corporation, in Herndon, VA.

Maj Gen Lawrence Stutzriem, USAF (Ret.), is the Mitchell Institute's research director, and an expert on modern combat aircraft operations, aerospace power, and national security affairs. Stutzriem served more than three decades in the US Air Force a fighter pilot, flying the F-4, F-16, and A-10. His assignments included directing air activity for Operation Southern Watch, and he was a member of the planning and operations team that spearheaded the initial air operations over Afghanistan as part of Operation Enduring Freedom. In his final assignment, he oversaw strategy, plans, and policy for North American Aerospace Defense Command (NORAD) and US Northern Command (NORTHCOM).

Heather Penney is a senior resident fellow at the Mitchell Institute, where she conducts research on defense policy. Prior to joining Mitchell, Penney worked over a decade in the defense industry, working on budgets, program execution, and campaign management. An Air Force veteran and pilot, Penney served in the Washington, D.C. Air National Guard flying F-16s and G-100s, and has also served in the Air Force Reserve in the National Military Command Center.