GOVERNMENT DATA RIGHTS CHALLENGES: Tips on How to Avoid & Respond

By Jonathan M. Baker,
Shawn Haque,
John E. McCarthy Jr.,
& Aaron Raddock

The basics of government contracts rights in technical data and computer software, the process the government uses to challenge a contractor's data rights assertions, and several business practices contractors can implement to be better prepared to avoid and respond to those challenges.

It was supposed to be a boon for the company.

The company had for years invested millions of dollars in its new product—a product that included novel hardware and thousands of lines of proprietary source code. The product was finally ready to go to market. The company was thrilled when it received a contract from the U.S. federal government, which included options for thousands of units. The company was expecting this contract to be a launching point for a long line of government business, including maintenance and sustainment of the product and its software. When selected for award, the company gladly signed the contract. Backs were patted and glasses were raised.

However, the government first wanted to make a few changes to the product. More specifically, the contract required the company to modify certain aspects of the hardware and tweak certain software modules to meet the government's specific needs. The company performed flawlessly, completing the customization and delivering to the government what the company deemed to be its proprietary technical data and computer software. Each delivery included the proper restrictive markings indicating that the delivery was subject to "limited rights" or "restricted rights," in accordance with the contract.

Two years later, however, a new contracting officer arrived on the scene. She mentioned during a status call that the government will not be exercising the contract's production options, but instead that it was considering holding a competition for the follow-on production units and the embedded software. Shortly thereafter, the government began questioning whether the restrictive markings the company placed on the delivered technical data and computer software were correct.

Then came the contracting officer's first letter. In that letter, the government asserted that even though the delivered technical data and software included markings designating them as proprietary and subject to "limited rights" or "restricted rights," the contract actually granted the government "unlimited rights," or, at a minimum, "government purpose rights," in those deliverables and asked the contractor to justify those restrictive markings. At that point, the government's intent became clear—it wanted to challenge the contractor's asserted restrictions to provide the technical data and computer software to the contractor's competitors to create competition for the production contract. Stunned because "everyone knew" that the product was proprietary, the company wondered...how should it respond to the contracting officer's letter?

The Government's Increasing Emphasis on Data Rights

More and more companies are facing similar situations each year. Historically, when a contractor asserted "limited rights," "restricted rights," or even "commercial" license rights in its technical data and computer software, the government rarely asked questions. However, more recently, the government, and in particular, the Department of Defense (DOD), has begun to aggressively pursue rights in technical data and computer software in an effort to increase competition and reduce costs, even where such rights determinations have been undisputed for years or even decades.

For example, DOD has touted a new initiative titled "Better Buying Power" (BBP) as a way to think more critically about procurements and maximize the value the government obtains from its investment. In the abstract, the BBP initiative seems to make sense: It encourages program offices to procure major systems with modular open system architecture to allow the government to compete future modifications and upgrades to those major systems at the component level. However, oftentimes a necessary predicate for this open system architecture is the acquisition of sufficient rights in data and computer software at a granular component level to allow for the integration of those components into a system. For acquisitions of entirely new major systems, that is arguably the price of doing business with the government. However, for existing major systems, BBP seemingly encourages contracting officers to also go after rights in existing technical data and computer software. This has manifested itself in multiple respects.

First, BBP encourages contracting officers to include terms in solicitations that require contractors to explain their approaches to open system architecture and data rights in their proposal, and agencies to evaluate the contractors' approaches to architecture and data rights as part of its source selection process. Contracting officers appear to be paying attention, as more and more of these provisions are appearing in DOD solicitations.

Second, DOD is also becoming more assertive in practice to ensure the government understands what rights it will have in an offeror's technical data and computer software. For instance, during contract formation, agencies appear to be placing increased scrutiny on the data rights assertions included in offerors' proposals. Nowadays, it is not uncommon for an agency to ask an offeror during discussions to clarify what rights in technical data and computer software the government will obtain as part of the offeror's proposed solution. And in some procurements, the government is even asking contractors to justify their asserted restrictions during the proposal process. Because more solicitations are including factors that require the agency to consider open system architecture and data rights during the evaluation, the offerors' responses to these discussion questions can make the difference between receiving the award and not.

Third, even post-award, the government is placing more emphasis on contractors' data rights assertions. Although we have not seen any empirical data regarding the number of times the government challenges a contractor's data rights restrictions, anecdotally such challenges appear to be on the rise. Contractors performing, or seeking to close out, contracts are increasingly faced with requests from agencies to provide data to justify the asserted restrictions on their technical data and computer software.

This increased focus on data rights means that careful contractors must proactively manage their data rights. More specifically, contractors must consider their data rights strategy early in the competitive process and must put in place mechanisms that will help them to avoid, prepare for, and respond to government data rights challenges.

Rights in Technical Data and Computer Software: The Basics

Before addressing techniques contractors may implement to avoid and respond to government challenges, it is important to understand some of the basic concepts governing rights in technical data and computer software. As an initial matter, in virtually all disputes concerning data rights, the issue is the license rights the contractor grants to the government in the technical data and computer software, not whether the government obtains title to the technical data or software. Under the standard *Federal Acquisition Regulation* (*FAR*) and the *Defense FAR Supplement* (*DFARS*) clauses, the contractor always retains title and the government gets a license. Thus, when the government challenges a contractor's data rights assertion, it is normally disputing the scope of the license given to the government—not whether the government "owns" the technical data or computer software. Contractors and agencies alike routinely conflate the concepts of data rights and ownership, which can lead to ambiguous contract language and unintended results.

Additionally, contractors should remember that delivery requirements and data rights are two distinct concepts. A contract's delivery requirements establish what products, services, technical data, and computer software the contractor is required to deliver to the government. The data rights provisions, on the other hand, address the rights in technical data and computer software the contractor is granting to the government, irrespective of the contract's delivery

requirements. In other words, the contract may require a contractor to deliver technical data (e.g., a drawing) to the government, but what the government is permitted to do with that technical data (e.g., how it may be used and to whom may it be disclosed) may be quite narrow. By contrast, a contract may grant the government very broad rights in technical data and computer software, but not require the contractor to deliver that technical data and computer software to the government. In that case, the government will have no ability to exercise its very broad rights because it will not even possess the technical data and computer software to which it has rights.

Types of Rights in Technical Data and Computer Software

Although the government and contractor can agree to unique data rights provisions, the rights granted to the government are usually spelled out in one of the standard *FAR* or *DFARS* contract clauses. For civilian agency contracts, the most common data rights clause is FAR 52.227-14, "Rights in Data—General." Covering both technical data and computer software, FAR 52.227-14 defines the various types of rights the government may obtain and explains when the government obtains them. The three basic types of rights the government may obtain include:

- **Unlimited Rights—**The broadest rights that may be granted to the government in technical data *or* computer software. They allow the government to, among other things, use or disclose the contractor's technical data and/or computer software for any purpose whatsoever. These rights also allow the government to permit others, including other companies, to do the same. In other words, with unlimited rights, the government can provide a company's technical data or computer software to one of the contractor's competitors and that competitor can use it for any purpose, including for any nongovernmental (i.e., commercial) purpose.

- **Limited Rights—**The most restrictive rights that may be granted to the government in *technical data*. With limited rights, the government may use or reproduce the technical data, but generally is prohibited from disclosing it outside the government or using it for manufacturing purposes.

- **Restricted Rights—**Refers to the most restrictive rights that may be granted to the government in *computer software* and include, among other things, the right to use or copy for use the software for the specific computer for which it was acquired.

In DOD procurements, under the standard data rights clauses (i.e., DFARS 252.227-7013 and DFARS 252.227-7014), the government may also acquire government purpose rights in technical data and/or computer software. Government purpose rights permit the government to use technical data and computer software within the government without restriction, and also authorize the government to release such technical data and computer software to third parties to use for government purposes, including, most significantly, reprocurement purposes. Government purpose rights revert to unlimited rights after a specified period of time—typically five years.

Allocation of Data Rights

In addition to defining the various types of rights the government may acquire in a contractor's technical data and computer software, the standard *FAR* and *DFARS* clauses also specify how those rights are allocated. Although there are important differences, which are beyond the scope of this article, the *FAR* and *DFARS* do share a common thread in this context. Both sets of rules allocate rights based, in part, on whether the computer software or the item, component, or process to which the technical data pertains was developed at private expense. If developed exclusively at private expense, the government normally obtains only limited rights (in technical data) or restricted rights (in computer software). If developed exclusively at government expense, the government will obtain unlimited rights. And for DOD procurements, if both government and private funds were used for development, the government will obtain government purpose rights.

It is this element of the *FAR* and *DFARS* rights allocation schemes that is oftentimes disputed. In proposals, contracts, and during contract performance, a company will often assert that it developed the item, component, process, or computer software at issue exclusively at private expense. The contractor marks its technical data and computer software with these restrictions and delivers them to the government. However, the government may disagree and allege that the restrictive markings are not appropriate because the contractor previously developed a part of the item, component, process, or computer software under some prior government effort. These allegations can quickly escalate from informal communications to a formal contracting officer's challenge to the contractor's data rights assertions.

The Anatomy of a Data Rights Challenge

The anatomy of a data rights challenge is relatively straightforward from a procedural standpoint. The *FAR* and *DFARS* contain standard clauses setting forth specific procedural requirements for the government to formally dispute the data rights assertions through the issuance of a contracting officer's "challenge." The challenge process for civilian agencies is set forth in FAR 52.227-14(e). DFARS 252.227-7037 addresses the procedures applicable to technical data and DFARS 252.227-7019 contains the procedures applicable to computer software for DOD. The *DFARS* provisions also specify procedures that allow the government to obtain information from the contractor concerning its data rights assertions on a more informal basis, commonly referred to as a "pre-challenge" request for information. Although the *FAR* does not include similar pre-challenge provisions, some civilian agencies will nevertheless commence informal discussions with the contractor in an effort to resolve the dispute prior to issuing a formal challenge.

Disputes typically begin with the agency issuing a pre-challenge request for information. As part of a pre-challenge, the contracting officer may ask the contractor to furnish a written explanation for any restriction on the government's rights to technical data or computer software that the company has asserted. After receiving the company's response, the contracting officer may issue follow-up requests for additional information.

If the contractor or subcontractor fails to respond to the contracting officer's pre-challenge request for information or the contracting officer determines that reasonable grounds exist to question the company's data rights assertions, and that continued adherence to the restrictive markings would create barriers to subsequent competitive acquisitions, the contracting officer may then formally challenge the validity of the company's technical data and computer software markings. The formal challenge must state the specific grounds for challenging the contractor's asserted restriction and give the contractor 60 days to respond. Upon the contractor's written request and showing that it needs additional time to submit a response, the contracting officer must extend this 60-day deadline.

If the contractor decides to respond to the contracting officer's data rights challenge, that response is considered a "claim" under the Contract Disputes Act, and therefore must be certified per FAR 33.207. As discussed in further detail later in this article, the contractor should ensure that its response addresses the specific issues raised in the challenge and that it provides copies of all relevant documentation supporting the contracting officer's asserted rights restrictions. It is important for the contractor's first challenge response to be thorough and complete because it may have limited, if any, opportunities to supplement its response, even on appeal.

A contracting officer typically has 60 days to issue a final decision sustaining or rejecting the validity of restrictive markings. If the contracting officer agrees with the contractor's data rights assertions, the government will continue to be bound by them. If the contracting officer rejects the assertions, the government will continue to be bound by the restrictive markings for a period of time to permit the filing and resolution of any appeal. If the contractor or subcontractor fails to appeal or file suit, the government may cancel or ignore the restrictive markings.

Practical Pointers for Avoiding and Responding to a Data Rights Challenge

Despite the appropriate use of restrictive markings, contractors may, as a result of the challenge process previously discussed, relinquish certain rights to intellectual property if they lack the ability to justify those restrictions. The government's heightened scrutiny of data rights assertions, and the increase in government challenges, has caused contractors to take further measures to protect intellectual property. After a challenge is initiated, or even much earlier

during the rush to respond to a solicitation, it is often too late to take preventative measures to protect data rights. Contractors are wise to think hard about what steps it can take now to avoid these situations in the future.

Whether a contract is successful in defending a data rights challenge normally depends on the adequacy of its documentation. While the circumstances of each government challenge are unique, contractors faced with a challenge will ideally have adequate proof to demonstrate what was developed outside a government contract at private expense and what was developed at government expense in the performance of a government contract. Reaching this point requires an understanding of two fundamental concepts.

The first concept for contractors to understand is what development funding is government money and what development funding is not government money. The *DFARS* defines the phrase *developed exclusively at private expense* as development that "was accomplished entirely with costs charged to indirect cost pools, costs not allocated to a government contract, or any combination thereof."[1] In other words, *private expense* includes direct contract charges on nongovernment contracts as well as indirect charges, such as independent research and development and bid and proposal funds, even though such charges may be recoverable, in part, under cost-type government contracts. By contrast, *government expense* is limited to direct contract charges for any aspect of the development effort.

The second key concept is known as the "doctrine of segregability." According to this doctrine, the determination of whether the item, component, process, or computer software at issue was developed using government or private funds should be made at the lowest practicable level of the item, component, process, or software.[2]

With those fundamentals in mind, contractors should strive to maintain records to support its data rights assertions for each segregable item, component, process, or computer software element. Indeed, under certain *DFARS* contract clauses, contractors are required to maintain evidence to support their restrictions on government data rights.[3] For example, for computer software, the *DFARS* states:

> The contractor shall maintain records sufficient to justify the validity of any markings that assert restrictions on the government's rights to use, modify, reproduce, perform, display, release, or disclose computer software delivered or required to be delivered under this contract and shall be prepared to furnish to the contracting officer a written justification for such restrictive markings in response to a request for information....[4]

Practical Techniques to Mitigate Risk

A contractor's ability to demonstrate that the development of its intellectual property was exclusively at private expense requires upfront planning, training, and ongoing diligence. Although there are a number of different ways to demonstrate private funding, some best practices include the following:

- **Document Project Scope**—Prior to beginning a new internal, privately funded development project, document the project scope and verify that it does not overlap with the scope of any existing government contract. Similarly, prior to accepting a new federal contract, confirm that its scope does not overlap with an existing internal development effort.

- **Use Separate Project Codes**—Each internal development effort should have a separate charge number that serves as a unique identifier. This allows for the tracking and collection of costs—both directly assigned and indirectly allocated to the specific development effort—and prevents development costs from being billed directly to a government contract. In cases of development involving mixed government and private funding, track development efforts to the lowest segregable level possible to retain the ability to assert restrictive rights at the subcomponent level.

- **Retain Cost Support**—All internal costs assigned to the unique internal project charge code should be supported with underlying documentation. Ideally, timecards from labor charges would contain narratives describing the work completed and the alignment with the internal development effort. Since this is often impractical, contractors may more realistically provide specific work authorizations associated with the internal project and/or maintain a detailed work breakdown structure identifying the key tasks performed. Additionally, purchase orders for any equipment or materials should align with the project's budget or procurement plan.

- **Date and Annotate Project Records**—Contractors should date and annotate key project records and outputs such as test reports, drawings, specifications, engineer notes, etc., with the applicable project code. This will provide a linkage between certain tasks and associated costs of the development effort, and also confirm that project milestones had been satisfied before the receipt of any government funds that may relate in some way to the developed item. One helpful method would be to annotate the technical records and/or software with the relevant charge code.

- **Educate Employees**—Key employees performing on the independent research and development project (typically engineers) need to understand the importance of tracking efforts and tasks. This is especially critical for those employees working on independent research and development projects and government contracts at the same time. Periodic training to instill this discipline is often beneficial.

- **Develop Policies and Procedures—** Contractors with significant internal development budgets should maintain policies and procedures covering topics such as project definition, budgeting, status reporting, key milestones, project costing, and overlaps with other projects. This will augment any training to key employees and help raise the importance and awareness of the employee's role/company's expectations in preserving intellectual property.

- **Establish a Point of Contact—** Engineers may have direct access to customers, but should not be the ones communicating with the government and/or prime contractors concerning deliverables. Avoiding these types of contacts will help ensure that restricted technical data and/or computer software is not provided to the government or the prime contractor if such delivery is not required by the terms of the contract. Companies should provide the technical staff a single point of contact for the communication of technical information.

- **Monitor the Scope of Development Efforts—**Ensure that the as-performed scope of work is consistent with the planned scope throughout both internal and contractual development efforts.

- **Update Record Retention Policies—** Develop a separate record retention policy related to key development records, or exclude such records needed to justify data rights assertions from the company's existing document destruction policies to ensure they are available in the event of a challenge.

Contractors often employ various information systems to help execute some of these recommendations. For example, contract management software may assist with the identification of any overlapping scope between internal development efforts and development under government contracts. A robust accounting system often plays the most important supporting role in facilitating the separate tracking of development costs.

For contractors performing cost-reimbursable work, the current accounting system should already possess the capabilities described herein to comply with existing contractual cost accounting requirements. In that case, the incremental effort to prepare for data rights challenges will still require highly disciplined use of the system, thoughtful documentation, clear policies and procedures, and routine training. However, for contractors performing solely on firm-fixed-price or other contract types, their accounting systems may lack important functionality needed to maintain appropriate records. Depending on the functionality in place and the magnitude of the risk, this may warrant anything from an accounting system enhancement or overhaul to a more robust set of memorandum books and records to document development efforts performed at private expense.

Conclusion

As the government looks for more ways to extend each taxpayer dollar and realize the full value under each government contract, contractors can expect to see continued efforts by agencies to push back on the contractors' data rights assertions. However, by carefully planning, executing, and documenting development efforts, contractors can be better positioned to defend against such challenges and maximize the value of their own intellectual property investments. **CM**

ABOUT THE AUTHORS

JONATHAN M. BAKER is a counsel for Crowell & Moring LLP.

JOHN E. MCCARTHY JR. is a partner with Crowell & Moring LLP.

SHAWN HAQUE is the corporate counsel for Accenture Federal Services LLC.

AARON RADDOCK, CFE, CFCM, is a senior manager with Baker Tilly Virchow Krause LLP/Baker Tilly Beers & Cutler PLLC.

Send comments about this article to cm@ncmahq.org.

ENDNOTES

1. DFARS 252.227-7013(a)(8).
2. *See* DFARS 227.7103-4(b), 252.227-7013(a)(8)(i), *and* 252.227-7014(a)(8)(i).
3. *See, e.g.*, DFARS 252.227-7019(b) *and* 252.227-7037(c).
4. DFARS 252.227-7019(b).