



Defense Contractors, Data Rights, and the “Right to Repair”

September 23, 2026

The U.S. Department of Defense (DOD) often relies on [private contractors](#) to support its mission. (DOD is using a “secondary Department of War designation” under [Executive Order 14347](#).) DOD works with these contractors to develop and field complex weapons systems that include technologies developed by the government, by private contractors, or by a combination of both.

Private companies may have intellectual property (IP) rights in technologies that they developed, which grants them exclusive rights in, for example, data and software. DOD may therefore need contractual permission (i.e., a license) to access data or modify software to conduct necessary maintenance and repairs.

A lack of DOD access to data may delay deployment of key DOD weapons systems and increase sustainment costs. For example, a 2026 DOD Office of the Inspector General (OIG) [review](#) of the [F-35 Joint Strike Fighter](#) (JSF) program found that DOD did not “enforce a contract requirement for Lockheed Martin to identify and provide accurate data on Government property within its possession.” [OIG stated](#) that “inaccurate and incomplete inventory data could have a negative operational impact on the program and may lead to uninformed logistical and budgetary decisions.”

Some [Members of Congress](#) and [analysts](#) are advocating for contractors to provide DOD access to technical data and software needed to repair and maintain acquired weapons systems. This stance is known as the *right to repair*.

IP and DOD Data Rights

[IP law](#) refers to various types of legal rights to exclude others from making, copying, or using intangible creations of the human mind. Generally, IP protections are [intended](#) to encourage innovation by providing incentives to generate new works and useful inventions. At the federal level, IP includes [four main types](#) of legal protection: patents, copyrights, trademarks, and trade secrets. These legal regimes each [protect](#) a distinct type of creation and grant the relevant IP owner rights that vary in scope and duration. For example, [trademarks](#) protect words and symbols used to identify the source of commercial goods and services, while [patents](#) grant inventors a “temporary monopoly” on new and useful technologies. (Patent rights in inventions developed with federal funding are generally governed by [the Bayh-Dole Act](#).)

The forms of IP of primary relevance to DOD’s right to repair are copyrights and trade secrets. [Copyrights](#) protect original works of authorship, including human-written software (i.e., computer code). Because copyright does not [protect](#) facts or unoriginal factual compilations, technical data is often protected by a different form of IP, [trade secrets](#). Either way, the creator of the software or the owner of the technical data may have the right to prevent others from [copying](#) or [accessing](#) the information without authorization, as a matter of IP law.

DOD uses the shorthand [data rights](#) to refer to the government’s IP [license rights](#) related to technical data and computer software. [10 U.S.C. §3013](#) defines *technical data* as “recorded information ... of a scientific or technical nature ... relating to supplies procured by an agency,” excluding computer software. For example, technical data can include equipment manuals, engineering drawings, and specifications. The Defense Federal Acquisition Regulation Supplement (DFARS) [defines computer software](#) as “computer programs, source code, source code listings, object code listings, ... and related material,” excluding databases.

Data Rights and DOD’s Right to Repair

For both DOD and the general public, IP protections can [impair](#) users’ ability to repair technology they have purchased, particularly for software-enabled devices. For example, a repair may require modification of a device’s software or access to maintenance data. (Nevertheless, IP is not [always](#) a barrier to repair or maintenance, and [many factors](#) beyond IP can impede one’s ability to repair.)

Because DOD systems “[are](#), and will be, increasingly dependent on technology” for their operation and maintenance, DOD asserts acquiring the “appropriate IP rights is vital for ensuring the systems will remain functional, sustainable, upgradable and affordable.” On the other hand, DOD acquisition of broader IP rights beyond what DOD assesses to be [necessary for maintenance and operations](#) may lead to deleterious secondary effects, including increased DOD contracting costs or the discouragement of private companies from working with the military. Thus, as [DOD’s Instruction on IP Acquisition and Licensing](#) notes, “balancing the interests of the U.S. Government and industry in IP can be difficult.”

DOD [policy](#) “requires fair treatment of IP owners, and seeks to create conditions that encourage technologically advanced solutions to meet DOD needs.” Current DOD guidance [urges](#) a strategic approach to IP acquisition early in a technology’s life cycle. This approach may use standard data rights terms or specialized contractual provisions tailored to balance DOD and industry needs.

Federal Procurement and Data Rights

The [Federal Acquisition Regulation](#) (FAR) provides several standard clauses for data rights in government contracts, which [apply](#) to all executive agencies *except* DOD. Although the standard FAR clauses do not apply to DOD, the terms and conditions provide a useful example of how civilian agencies approach IP acquisitions. The FAR [notes](#) that “generally, a contract should contain only one data rights clause,” but it allows for more than one clause if needed.

Generally, the FAR [standard clauses](#) give the government *unlimited rights* to data first produced under a government

contract (that is, produced at government expense), and for certain types of key data, including manuals and form, fit, and function (FFF) data. With [unlimited rights](#), the government can use, modify, and reproduce such data “in any manner and for any purpose” and authorize others to do so as well.

For data and software “developed at private expense,” FAR [authorizes limited rights](#), where the contractor may [withhold](#) the data from the government and provide FFF data instead, or deliver that data with restrictions on the government’s right to reproduce or disclose it.

DOD and Data Rights

For DOD, the [DFARS](#) provides [eight standard](#) data rights licensing provisions. The relevant standard clause [depends](#) on several factors, including who developed the data and software, and whether the data or software are commercial products. (These provisions do [not](#) apply to non-FAR agreements such as [other transactions](#).)

Under these provisions, DOD [generally](#) gets unlimited rights in data and software developed “exclusively with Government funds,” as well as some specific categories of data such as FFF and data necessary for operation, maintenance, installation, or training (OMIT data). For purely privately developed data or software, government data rights [may](#) be limited or restricted. For data and software developed as a partnership between the contractor and DOD (“mixed funding”), the department may use specially negotiated provisions, or DOD may retain [government purpose rights](#), whereby the government may use and reproduce the data [for governmental activities](#) but may not disclose it for commercial purposes.

[10 U.S.C. §3791](#) requires that DOD “develop policy on the acquisition or licensing of intellectual property” in part “to encourage customized intellectual property strategies for each system based on, at a minimum, the unique characteristics of the system and its components.”

Additionally, DOD’s office of Acquisition and Sustainment (A&S) maintains an “[IP Cadre](#),” which “leads a coordinated DOD-wide effort to modernize IP policies, culture, and best-practices.” It “serves as a focal point” on IP issues between DOD and the private sector, including “hosting an ‘enhanced engagement’ ... approach to revise the [Defense Federal Acquisition Regulation Supplement (DFARS)] IP coverage with industry input.”

Technical Data and Major Defense Systems

DOD is to follow specific statutory requirements for [major defense acquisition programs](#) (MDAPs), the most expensive and technically complex category of defense acquisition programs. [10 U.S.C. §4324](#) requires that DOD develop “an intellectual property management plan for product support” for all MDAPs before beginning the [engineering and manufacturing development](#) phase.

Additionally, [10 U.S.C. § 3774](#) requires that MDAP program managers “assess the long-term technical data needs” of their

program and “establish corresponding acquisition strategies that provide for technical data rights needed to sustain such systems and subsystems over their life cycle.” MDAP program managers are to develop such assessments [before](#) soliciting bids for contracts. These assessments [are to](#) “address the potential for changes in the sustainment plan over the life cycle of the weapon system or subsystem.”

Data Rights and the Defense Industrial Base

DOD’s approach to technical data rights, as discussed above, may be constrained by legal limitations. Nevertheless, DOD’s approach to IP may also have implications for the defense industrial base (DIB). Some analysts, including some affiliated with defense industry, [assert](#) that DOD’s “access to innovation is weakened when companies are at risk of losing sensitive, proprietary [IP].” Others [contend](#) that allowing contractors to maintain exclusive data rights or access to maintenance information limits competition within the DIB by creating “artificial, anticompetitive barriers that force the military to rely on original equipment manufacturers for sustainment operations.”

Congressional Efforts to Enhance DOD Data Rights

Some members of Congress have expressed interest in DOD technical data rights. In 2024, for example, Senator Warren introduced [S. 5497](#), the Servicemember Right-to-Repair Act of 2024, which would have required that contractors provide DOD “fair and reasonable access to all the repair materials, including parts, tools, and information.” Representative Perez introduced a companion bill, [H.R. 10401](#), in the House. In 2025, Senators Warren and Sheehy introduced a similar measure, [S. 2209](#), the Warrior Right to Repair Act of 2025; Representative Perez introduced a companion bill of the same title, [H.R. 5155](#), in the House.

Issues for Congress

Congress may consider whether or not current statutory requirements concerning DOD’s technical data allow DOD efficiently and effectively to conduct maintenance and repairs. Congress may also consider whether or not to increase its oversight activities on the subject of data rights, including over certain MDAPs.

Section 861 of the House-passed version of a Fiscal Year 2027 National Defense Authorization Act (NDAA; [H.R. 8800](#)) would require that data rights in DOD contracts default to government purpose rights, unless the contractors clearly establish a need for more restrictive rights. It would also require that DOD study the feasibility of recovering “excess payments” it may have made to contractors due to “unjustified restrictions on technical data.”

Alexandra G. Neenan, Analyst in U.S. Defense Policy
Kevin J. Hickey, Legislative Attorney

IF13320

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS’s institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.