# The Pros And Cons Of The Senate's DOD Data Rights Plan

By **Tyler Evans and Anna Menzel** (August 31, 2023)

Tyler Evans

Anna Menzel

The U.S. Senate's version of the annual National Defense Authorization Act includes a provision that large businesses will likely celebrate and small businesses will come to hate.

After over three decades of regulations stating the contrary, the Senate is finally proposing to clarify that the U.S. government should not automatically obtain unlimited rights in government contractor data that is necessary for operation, maintenance, installation or training — or OMIT data — purposes.

At the same time, however, the Senate is proposing to expand the U.S. government's rights in detailed manufacturing or process data when a contractor — likely a small business — is deemed unable to meet the U.S. government's needs.[1]

**New Protections for OMIT Data**

The current framework for OMIT data was established through a series of events beginning in 1986 when Congress passed a statute allowing contractors to prohibit the U.S. Department of Defense from disclosing privately funded data to third parties, including other contractors.[2]

The statute excluded OMIT data from this prohibition to the extent it did not also constitute detailed manufacturing or process data, which could occur, for example, when a maintenance manual includes instructions on assembly.

When establishing and implementing regulations, the DOD had the option of requiring contractors to provide to the government purpose rights in OMIT data, which would have generally only permitted the data to be used within the U.S. government and by third parties in performing government contracts.

However, the DOD ultimately went further and provided the U.S. government with "unlimited" rights in OMIT data, which permitted it to be publicly disclosed and used by third parties in commercial business.[3]

The DOD first envisioned that these rights would have a limited impact because they initially only applied to manuals and instructional materials that were specifically required to be delivered or prepared under a contract.[4]

However, in 1994, the DOD established the current framework by extending these rights to any OMIT data, regardless of whether it was prepared in commercial business completely independent of a government contract.[5]

This change had a significant impact on federal contractors because the U.S. government could now obtain unlimited rights in a contractor's commercial operational, maintenance, installation and training materials simply because a contractor agreed to sell a product or service to the DOD.

For example, under the current framework, a company that maintains a commercial business servicing aircraft engines or computer software needs to provide the U.S. government with unlimited rights in maintenance manuals for those engines or operating instructions for that software simply because the contractor agreed to provide similar services to the DOD.

This result can occur even when the U.S. government is otherwise required to receive reduced data rights, such as when a contractor provides a commercial item or performs work under the Small Business Innovation Research program.[6]

Moreover, the U.S. government does not need to exercise its unlimited rights to trigger negative consequences for a contractor. The sheer act of granting another party like the U.S. government unlimited rights to use and disclose data for any purpose is inconsistent with an intent to keep the data confidential and likely destroys trade secret protections.[7]

Thus, if a competitor receives proprietary OMIT data in which the U.S. government has unlimited rights, the competitor would likely be able to use the data for its commercial business without worrying about misappropriating trade secrets.[8]

The DOD has also taken steps to limit a contractor's ability to rely on other forms of intellectual property to prevent competitors from using OMIT data in their commercial business. For example, the DOD has successfully maintained that a contractor cannot place a copyright notice on OMIT data in which the U.S. government has unlimited rights.[9]

As a result, competitors can potentially claim innocent infringement if sued for violating a contractor's copyright.[10] The DOD's position would also likely extend to patents, trademarks, mask works and vessel hull designs, with a similar effect of limiting a contractor's ability to protect its intellectual property.[11]

Accordingly, although the DOD is expressly prohibited from impairing a contractor's intellectual property, its insistence on receiving unlimited rights in OMIT data has long had this effect and directly harmed the commercial business of its contractors.[12]

Fortunately, the Senate is now proposing to change this result by revising the statute that initially led to the current framework. Specifically, the Senate is proposing to clarify that the U.S. government by default can only obtain government purpose rights in OMIT data, which would prevent the DOD from continuing to insist on receiving unlimited rights.[13]

The DOD would presumably still be able to insist on having rights in OMIT data produced completely independent of a government contract — which is itself a questionable interpretation of the applicable statute and inconsistent with how civilian agencies handle this issue.[14]

However, the Senate's proposal would at least establish a sensical framework under which OMIT data could be used within the U.S. government and by third parties in performing government contracts without destroying or limiting the value of the data for a contractor's commercial business.

**Reduced Protections for Detailed Manufacturing or Process Data**

In contrast, the Senate's proposal would reduce contractor rights in detailed manufacturing or process data, which covers an even more valuable set of conditions, formulas,

specifications, drawings and steps needed to produce an item or perform a process.

For good reason, the U.S. government has historically not had the right to use a contractor's privately funded manufacturing or process data to produce competing products or components. However, under the Senate's proposal, the U.S. government would now be able to disclose detailed manufacturing or process data to competing contractors as needed for operations, maintenance, installation, or training in support of wartime or contingency operations.

To do so, an agency would just need to determine that the contractor initially possessing the data would be "unable to satisfy military readiness or operational requirements for such operations," according to the NDAA.[15]

This change would likely have a disproportionate impact on small businesses, especially those that provide cutting-edge technology with defense applications. The DOD has a history of trying to transition a small business's novel technology to large contractors based on a belief that they can bring it to the field faster or cheaper than the initial developer.[16]

Thus, if a small business develops a new unmanned aerial vehicle or method for manufacturing semiconductors, and receives a related award from the DOD, the Senate's proposal would permit an agency to share that contractor's detailed manufacturing or process data with large contractors as long as the agency can make the case that doing so is necessary to support wartime or contingency operations.[17]

The agency could take this step even if the data was either privately funded or developed under enhanced data rights protections, such as those applicable under the Small Business Innovation Research program.

A small business would also likely have difficulty challenging the agency's determination due to the significant legal resources that would be required to do so, as well as the judicial and administrative deference that would likely be provided to the agency on a matter of national security.

Moreover, that the detailed manufacturing or process data could only be used in support of wartime or contingency operations would likely not be a significant limitation under this framework. A wide variety of circumstances can constitute contingency operations, and the determination of what constitutes a contingency operation is largely left to the discretion of the DOD.[18]

For example, based on the original emergency declaration for the 9/11 attacks, any DOD activity relating to a terrorist threat could likely still be deemed to involve contingency operations.[19]

In addition, work relating to national disasters and similar emergencies, such as the COVID-19 pandemic, could qualify.[20] That the U.S. government's rights would be triggered if data merely supports contingency operations also further expands eligible circumstances.[21]

For example, the government's rights could be triggered for manufacturing needs covering nonoperational maintenance, installation or training activities in the U.S. government.

As a result, the Senate's proposal would effectively give the DOD a statutory basis on which to continue its prior behavior of disregarding small businesses once they have developed a

technology that the DOD wants to quickly deploy or put into production.[22]

The DOD already has statutory authority to take data when necessary for national security purposes.[23] However, unlike this existing authority, the Senate's proposal would go further and give the DOD rights in detailed manufacturing or process data without compensating the data's initial developer.

The Senate should be lauded for finally addressing the DOD's aggressive position on OMIT data. However, the risk that the Senate's proposal would pose to small businesses with respect to detailed manufacturing or process data may ultimately outweigh the benefit of any fix to OMIT data.

---

*Tyler Evans is a partner and Anna Menzel is an associate at Steptoe & Johnson LLP.*



[1] National Defense Authorization Act for Fiscal Year 2024, S. 2226, 118th Cong. §868 (July 27, 2023).

[2] See Pub. L. No. 99–500, 100 Stat. 783, 1783-170 (Oct. 18, 1986).

[3] See 52 Fed. Reg. 12,390, 12,405 (Apr. 16, 1987); 52 Fed. Reg. 2,082, 2,085 (Jan. 16, 1987).

[4] Under prior data rights frameworks, DOD similarly only insisted on obtaining unlimited rights in OMIT data that was delivered to the U.S. government under a contract. See, e.g., 30 Fed. Reg. 6,965, 6,969 (May 25, 1965).

[5] 59 Fed. Reg. 31,584, 31,588 (June 20, 1994).

[6] See, e.g., DFARS 252.227-7015(b)(1)(iv); DFARS 252.227-7018(b)(1)(ii).

[7] See Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002, 1011 (1984); see also Thomas v. Union Carbide Agri. Prods. Co., 473 U.S. 568, 584 (1985); Sheets v. Yamaha Motors Corp., 849 F.2d 179, 183-85 (5th Cir. 1988); Conax Fla. Corp. v. United States, 824 F.2d 1124, 1128 (D.C. Cir. 1987).

[8] See, e.g., L-3 Commc'ns Westwood Corp. v. Robichaux, No. 06-279, 2008 WL 577560, at *6 (E.D. La. Feb. 29, 2008); HiRel Connectors Inc. v. United States, No. CV01-11069, 2005 WL 4958589, at *4 (C.D. Cal. Jan 4, 2005).

[9] See FlightSafety Int'l Inc., ASBCA No. 62659, 23-1 BCA ¶38245 (2022).

[10] See 17 U.S.C. §401(d).

[11] See 35 U.S.C. §287; 17 U.S.C. §§907, 909, 1306-07.

[12] See 10 U.S.C. §3771(a)(2) (expressly prohibiting DOD from implementing regulations

that impair a contractor's patents, copyrights, or other rights established by law).

[13] National Defense Authorization Act for Fiscal Year 2024, S. 2226, 118th Cong. §868 (July 27, 2023).

[14] See FAR 52.227-14(b)(1)(iii) (only providing rights in similar data when delivered under a contract).

[15] National Defense Authorization Act for Fiscal Year 2024, S. 2226, 118th Cong. §868(2)(C) (July 27, 2023).

[16] See, e.g., Night Vision Corp. v. United States, 68 Fed. Cl. 368 (2005), aff'd, 469 F.3d 1369 (Fed. Cir. 2006).

[17] The originator of the data would have some protection from large contractors using detailed manufacturing or process data for commercial business. However, it may be difficult for a small business to identify a large contractor's unauthorized use of such data, and large contractors would not be able to unlearn the data when improving their own products and services.

[18] See 10 U.S.C. §101(a)(13).

[19] See, e.g., 87 Fed. Reg. 55,897, 55,897 (Sept. 12, 2022).

[20] See Announcement Defense Pricing and Contracting, Office of the Under Secretary of Defense (Acquisition & Sustainment, Coronavirus Disease 2019 (COVID-19) Emergency Acquisition Flexibilities – Contingency Operation, available at https://www.acq.osd.mil/asda/dpc/docs/covid-19/COVID-19_Contingency_Operation_Information_Release_4.15.2020.pdf.

[21] See, e.g., O'Farrell v. Dep't of Def., 882 F.3d 1080, 1087 (Fed. Cir. 2018) (finding that a civilian attorney performing work at the Naval Surface Warfare Center in California was performing services in support of contingency operations in Afghanistan).

[22] See Night Vision Corp., 68 Fed. Cl. at 376.

[23] See 15 C.F.R. §§700.8, 700.13, 700.31 (granting the right to demand any "technical information, process, or service" pursuant to the Defense Production Act).