2012 Defense Act Could Weaken Contractors' IP Rights

By **Dietrich Knauth**

Law360, New York (February 27, 2012, 2:58 PM ET) -- In an effort to increase competition among defense contractors, Congress has given the U.S. military more leeway to demand technical data that is used to design the weapons it purchases, but the broad and ambiguous wording of the law could leave contractors scrambling to protect their intellectual property rights, experts say.

The government already had broad rights to contractor technical data that is developed with government funds. But the 2012 National Defense Authorization Act expanded the government's ability to demand technical data that is developed entirely with private funds, if the U.S. Department of Defense decides that the information is necessary to integrate or segregate a certain portion of a weapon or system.

Military leaders felt that the broader authority was needed to prevent contractors from segregating funds for a particular crucial component within a larger system, which would force the government to return to the same contractor if it wanted to buy more of the weapon system or upgrade already-purchased inventory. Rather than let contractors hold them over a barrel in procurement negotiations, contracting officials can use the new authority to segregate and work around the portion that contractors have kept as their own intellectual property.

But Congress may have used broader language than was needed to achieve that goal, creating consternation in the defense industry despite explanations from DOD and Senate Armed Services Committee attorneys who characterized the changes as minor, according to Ralph Clarke Nash Jr., professor emeritus at George Washington University Law School.

"The intent of the statute was to allow [contractors] to keep the proprietary rights in the segment of the system that they had, but to force them to release enough data so that they couldn't block competition on the rest of the system," Nash said. “If the statute says what they say it means, it doesn't have a very significant impact.”

Nash said the government's explanation will likely not be put into the regulations, and he suspects that the forthcoming DOD regulations will use essentially the same language as the NDAA.

Simply plugging the NDAA's language into the DOD regulations, expected to be published in March, could be troublesome, because the language is “not a model of clarity,” said John E. McCarthy Jr., a partner in Crowell & Moring LLP's government contracts practice.

“Companies can spend millions of dollars on developing their intellectual property, and they want clarity on whether or not they can retain that IP,” McCarthy said. “If the regulations attempt to push the envelope, its going to be very troublesome for many contractors.”

The NDAA says the U.S. “may require at any time the delivery of technical data that has been generated or utilized in the performance of a contract, and compensate the contractor only for reasonable costs incurred for having converted and delivered the data in the required form,” if the government determines that the requested data “is necessary for the segregation of an item or process from, or the reintegration of that item or process (or a physically or functionally equivalent item or process) with, other items or processes.”

Those sections contain two key ambiguities that could cause headaches for contractors, attorneys said.

First, it may not be clear what data or how much data will be required to segregate a system — and contractors are bound to fight with the government over the scope of such requests when they get them.

"It's almost like you're unplugging a widget and you need to know what all the various connecting parts are to reconnect to a new system,” said Holly Roth, a partner at Manatt Phelps & Phillips LLP. "It could be very, very, very complex.”

"When you get into the real world, the contractor would deliver a package of data, then the government will say that's not enough,” Nash said. “I don't think the government people will be able to define precisely what they'll be asking for. I don't know that anybody knows exactly what data they're talking about."

Second, attorneys raised concerns about the potential broadness of “utilized in the performance of a contract.” Taken to an extreme, that phrase could lead to absurd interpretations, such as requiring the source code for Microsoft Word, if a contractor used that program during a contract, attorneys said.

Louis Victorino, a partner at Sheppard Mullin Richter & Hampton LLP, called the inclusion of “or utilized” in the wording “insidious,” because it reaches beyond data developed at the government's expense.

"This suggests the government can require any data,” Victorino said. "This is, to me, the really, really important provision. This is a major expansion, and I hope that they didn't really mean to do what they're saying."

Fernand A. Lavallee, a partner with DLA Piper, said he suspects the language was purposely ambiguous, in order to give the DOD significant discretion in crafting regulations to implement the law. But the DOD could achieve the same results by simply doing a better job of defining its data needs and by demanding segregation and reintegration data from contractors at the start of a contract, he said.

"They're creating a solution to a problem that doesn't exist," Lavallee said. “If it's upfront, contractors can decide if they're comfortable offering that level of data. The ones that would have played the game of holding the government hostage would have already exited the process."

While the reintegration data will be protected by nondisclosure agreements, contractors are wary about disclosing information that could harm their businesses if the provisions are applied broadly or misunderstood. The DOD can turn over such data to other contractors in the effort to build around a proprietary system, which always carries risks, attorneys said.

"[The DOD] can take the intellectual property for company A and can now give it to company B, perhaps your competitor, and let them integrate it into their product," Victorino said. "There is always that risk that once that other company learns the 'secret sauce' or learns how the company solved the problem, they will find a way to use that."

The statute is not clear on whether the disclosure agreement would be between the contractor giving up the data and the contractor receiving it, or between the government and the contractor receiving the data. If it were the second case, a contractor could only sue the government for a potential breach of the nondisclosure agreement, and such cases are difficult to prove, according to attorneys.

While the rule is intended to create more competition by ensuring that the DOD can turn to a new group of contractors if a key company decides to stop working with the government, goes out of business or doesn't like the government's terms, it could have the opposite effect, Roth said. Demanding so much information could scare some companies away from even competing for contracts, according to Roth.

"I think it could have a chilling effect," Roth said. "Now that the government has the right to force me to give that information up to them, I'm going to think twice about the type of data that I might propose for use in any type of contract with the government."

David W. Burgett, a partner at Hogan Lovells, said that while contractors are right to be wary of the changes, the law, as written, appears to protect contractors from the worst exploitation of their intellectual property. The government will not be able to use that data to manufacture or re-procure a proprietary component; it can only use the data to eliminate the component, he said.

The government already has the authority to demand similar data under an existing provision for emergency repair and overhaul of a system, according to Burgett. Rather than a dramatic expansion of the government's data rights, the changes allow the government to protect itself from mistakes, such as not asking for needed data before or during a contract, Burgett said.

"Traditionally, the data delivery requirements would be specified in the contract. What I think the department is doing, is that they want to ensure that they can get data that they think they need even after the contract is finished," Burgett said. "Looking at the big picture, I wouldn't characterize any of these changes as being a large change in and of themselves."

While the DOD's regulations will shed some light on how far the military will go in pushing for new data access, the new rules will be part of a trend of contractors giving up more data.

Ralph Nash, who has been working in government contracts for 50 years, sees the new provisions as part of the "steady erosion of contractors' ability to protect his data in the first case." The government cannot force a contractor to give up data rights, but by using data rights as part of its evaluation of competing contract bids, it can leverage its buying power to get more and more data, he said.

"You could always buy data rights, but you had to buy them as a separate procurement," Nash said. “[Government agencies] have been, in the last five years, busily finding ways to use that competition to get data rights by treating it as something they're going to evaluate in selecting the winner of the competition."

Congress has taken an increased interest in data rights in recent years, creating confusion by quickly enacting new legislation — and sometimes withdrawing or changing rules “even before the ink's dry” on a law, Lavallee said.

"For the fourth consecutive year, Congress has issued another significant change in direction to defense contractors and to the DOD in the area of data rights," Lavallee said. ”That creates a continuation of a state of change, of unpredictability, which is necessarily a challenge for both the government and for the contractors."

--Editing by Lindsay Naylor.