SBIR·STTR
America's Seed Fund™
POWERED BY SBA

COURSE 9, TUTORIAL 2

WHAT ARE SBIR DATA RIGHTS AND WHY ARE THEY IMPORTANT?

SBIR/STTR Data protection is one of the most unique and important protections accorded Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) firms. These protections apply to all phases of the SBIR and STTR programs. Please note that throughout the balance of this discussion I may sometimes reference only SBIR, but that is for convenience only. Everything that I mention applies equally to the STTR program as well. One of the most important of these protections is that the government cannot disclose SBIR Data outside of the government.

The government receives a limited nonexclusive license, or right to use, SBIR Data, but such use cannot include disclosing it in any way. This nondisclosure obligation is accompanied by a Data Rights protection period. In its May 2, 2019 SBIR/STTR Policy Directive, SBA changed the Data Rights protection period for both SBIR and STTR funding agreements to a uniform 20-year period that begins on the date of award. This start date for the protection period is new, as is the 20-year period. The protection period no longer begins on the date of delivery of the last funding agreement deliverable. In exchange for the grant of the 20-year protection period, SBA eliminated the extension or "roll-over" provision, effective May 2, 2019. Thus, subsequent SBIR/STTR funding agreements no longer extend data protection periods for prior awards to the end of the protection period that applies to the current award. The 20-year protection period applies both to SBIR and STTR awards. Keep in mind that a Phase III award is by definition not paid for with Phase I or II SBIR/STTR funding. To get the most out of your participation, it is important that you re-align your marketing schedule to this new 20-year protection period for each award.

THE IMPORTANCE OF NONDISCLOSURE

These SBIR/STTR Data Rights protections have many implications. First and foremost, this nondisclosure obligation means that the government cannot compete technologies containing SBIR Data. Any such competition would mean disclosing the SBIR Data in solicitations, which the government cannot do. This unique right also underlies and supports the sole source Phase III mandate – the requirement to award Phase III awards to the SBIR developing firm to the greatest extent practicable. This single right – and obligation of the government – creates value in the SBIR firm and ultimately wealth for the SBIR owners.

Because of the importance of SBIR/STTR Data in the new program, it is vital for small businesses to understand the nature of SBIR Data and how to protect it. It is important to understand what SBIR Data is, as well as what it is not – so

that SBIR owners and their employees can better protect their technologies and SBIR Data. As we go through this analysis, one can quickly see that the SBA Directive treats SBIR and STTR Data alike.

WHAT IS SBIR/STTR DATA?

SBIR/STTR Data has three basic attributes: 1) it is recorded information, 2) of a technical nature, 3) that is generated under an SBIR or STTR funding agreement and appropriately marked with the SBIR/STTR Data Rights legend. We use the term "funding agreement" because SBIR awards can be grants, contracts, cooperative agreements, or any other type of funding award the government chooses to make.

> **SBIR/STTR Data has 3 essential attributes**
>
> **(1) It is recorded information**
> **(2) It is technical in nature**
> **(3) It is generated under an SBIR or STTR funding agreement, and appropriately marked**

Let's take a look at these three elements one at a time. First, SBIR/STTR Data must be recorded information. That is, SBIR Data must be reduced to writing and contained in a written document. SBIR Data can be source code, sketches, drawings, formulas, equations, reports, descriptions of SBIR technologies, SBIR final reports, and any other type of writing that meets all three of these criteria. SBIR Data protections, however, do not apply to ideas or concepts, unless those ideas or concepts are reduced to writing. SBIR Data protections protect the ideas contained in a written document, but not the idea itself without the writing. In order to protect an idea or concept outside of the written description of it one must resort to patent protection. Thus, the nondisclosure protection does not protect ideas or concepts by themselves. In general, most SBIR/STTR firms protect software and source code through this nondisclosure obligation, because they do not wish to disclose their software architecture or actual source code in a patent.

Second, SBIR Data must be technical in nature. Non-technical data does not qualify as SBIR Data. Cost and pricing information is a good example of this. This data is protected by the Freedom of Information Act, paragraph (b)(4), which constitutes an exception to mandatory disclosure of information by the government. It also can be subject to and protected by the Privacy Act. But the SBIR nondisclosure obligation of the government does not extend to such information. Such proprietary data is protected by these other means. Other non-technical information, such as background data on the company, is also not protected, and should be disclosed carefully and with that knowledge in mind. The test for this "technical" requirement is that it must relate somehow to the SBIR technology being developed in Phases I, II, and III. Therefore, this SBIR Data will be something

that the SBIR firm will seek to protect. Information or data that the SBIR firm advertises on its web site is not something it feels it must protect. This could include general descriptions of its SBIR technologies that do not give up trade secret information about the technology.

Third, SBIR Data must be generated under an SBIR or STTR funding agreement. Proprietary data that the firm developed with its own private funds is not SBIR Data. It was not developed under an SBIR award. It is protected by other means, as described above. Proposal information is also not SBIR Data, although the proposal may contain SBIR Data that was generated under prior SBIR funding agreements and is protected under them. Different laws and regulations protect proposal information and prevent its disclosure. Additionally, if SBIR Data is mixed so thoroughly with non-SBIR Data that the two types of data cannot be pulled apart, or severed from each other, then the whole body of data, including the non-SBIR Data, becomes subject to the government's non-disclosure obligation. This occurs often with respect to source code and computer software. Finally, the new May 2, 2019 Directive makes it clear that to qualify for Data Rights protection, the SBIR/STTR Data must be correctly marked. A grace period provides for the opportunity to correct a failure to mark or inaccurately marked SBIR/STTR Data within six months. This grace period is new and is shorter than an indefinite grace period in the prior Directive.

> **"Non-technical data does not qualify as SBIR/STTR Data"**

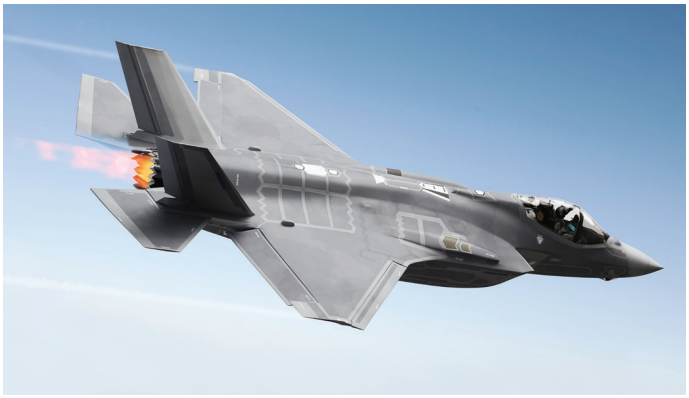
DIFFERENCES BETWEEN CIVILIAN AND MILITARY CLAUSES

Marking SBIR Data with precisely the wording set forth in the new May 2, 2019 Directive that applies to both civilian and military agencies is critical. Placing these legends on SBIR Data provides notice to federal employees handling such data that they cannot disclose it. Failure to mark data properly can lead to disclosure by the government of SBIR Data. The exact legend provided in the new Directive, once the agencies implement it, should be included on the title page or front page of the SBIR/STTR document or deliverable. At the bottom of each subsequent page, state:

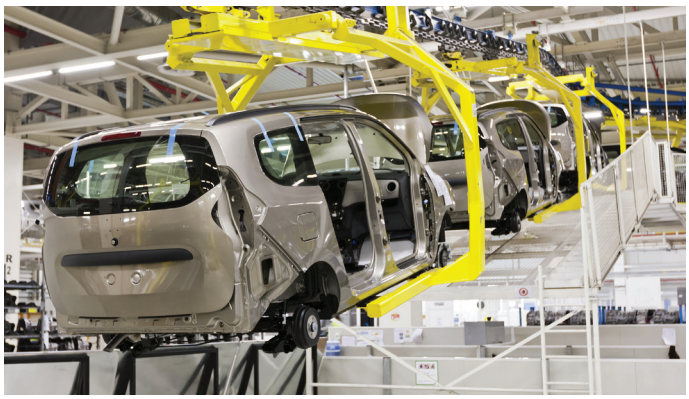
> **"This page is protected by and subject to the SBIR Data Rights legend set forth on the title page."**

The new combined Data Rights clause is the same for both SBIR and STTR funding agreements. The new clause implements a 20-year protection period (that does not include the extension or "roll-over provision) and applies to both civilian and military agencies. It provides for a date certain to be inserted in the header of the clause that is 20 years from the date of award of the SBIR or STTR funding agreement (changed from the date of the last deliverable from the prior directive). Because the new combined SBIR/STTR Data Rights clause is so different from the existing clauses—FAR 52.227-20 and DFARS 252.227-7018—it is vital that SBIR/STTR awardees check their funding agreements before signing them to ensure the agency has included these revisions in the proposed agreement. Inclusion of the existing FAR or DFARS clauses without the extension provision could result in an SBIR/STTR Data Rights protection period of only four or five years, respectively. Agencies should include special language that acknowledges and affirms application of the new Data Rights clause and the May 2, 2019 SBA SBIR/STTR Directive to the funding agreement, notwithstanding contrary provisions in the FAR or DFARS clauses, until they are amended. Failure of the agency to do so should be reported immediately to SBA.

IMPORTANT SBIR/STTR CLAUSES



DFARS clause 252.227-7018 for defense



FAR clause 52.227-20 for civilian agencies

THE IMPORTANCE OF MARKING DATA

Marking SBIR Data is critical to protecting it from government disclosure. Because the government cannot disclose SBIR or STTR Data, an SBIR firm's competitors can obtain such data only if they purchase the technology or acquire the SBIR firm. Be very careful not to disclose your SBIR Data voluntarily. If you make a PowerPoint presentation to the government, mark it with the SBIR Data Rights legend. Make certain that everyone in the room is with the government when you make the presentation. When in doubt, protect your data by marking it. When larger firms seek access to SBIR technologies, they many times pay premiums in the marketplace solely to obtain access to these SBIR technologies. Marking and preserving SBIR Data is the first step in creating such a premium value in the SBIR firm and its SBIR technologies.

POWERPOINT PRESENTATIONS

It is important in protecting SBIR Data to know what it is and what it is not. The caution not to disclose SBIR Data in PowerPoint presentations does not mean that a firm cannot make PowerPoint presentations at all or discuss an SBIR/STTR funded technology publicly. Far from it. Rather, firms must be careful about the level of technical detail they put into such presentations, especially if they are made publicly. Statements about the capabilities of the technology, when fully developed, are certainly acceptable. Comparisons to other existing technologies are acceptable. Disclosure of test results, especially if favorable, are acceptable and should even be encouraged. However, disclosing the specifics of sketches, drawings, equations, source code and code structure, final reports, how the technology works at the technical level, and so forth would constitute a voluntary disclosure of SBIR Data and should be avoided. It is the "technical" aspect of the definition discussed above that renders SBIR Data trade secrets that must be protected. When in doubt, the rule for owners and staff should be: "Don't disclose."

We hope this information on SBIR and STTR Data was helpful.

Prepared by
David Metzger, Esq.

TO LEARN MORE ABOUT THIS TOPIC
SBIR.GOV/TUTORIALS
REVISED JULY 2019