PGI Part 227 - TECHNICAL DATA AND ASSOCIATED RIGHTS

PGI 227.71 - TECHNICAL DATA AND ASSOCIATED RIGHTS

PGI 227.7103 Other than commercial products, commercial services, or commercial processes.

PGI 227.7103-2 Acquisition of technical data.

PGI 227.7104 Contracts under the Small Business Innovation Research Program and Small Business Technology Transfer Program.

PGI 227.7104-1 Policy.

PGI 227.7104-2 Rights in SBIR or STTR data.

PGI 227.72 - COMPUTER SOFTWARE, COMPUTER SOFTWARE DOCUMENTATION, AND ASSOCIATED RIGHTS

PGI 227.7200 Scope of subpart.

PGI 227.7203 Other than commercial computer software and other than commercial computer software documentation.

PGI 227.7203-2 Acquisition of other than commercial computer software and computer software documentation and associated rights.

Parent topic: PGI Defense Federal Acquisition Regulation

PGI 227.71 - TECHNICAL DATA AND ASSOCIATED RIGHTS

PGI 227.7103 Other than commercial products, commercial services, or commercial processes.

PGI 227.7103-2 Acquisition of technical data.

(b)(1) See DoDI 5010.44, Intellectual Property (IP) Acquisition and Licensing, sections 4.1 and 4.2, when formulating business advice and contract implementation strategies regarding the program manager’s tailoring of technical data requirements to the needs of the Government.

PGI 227.7104 Contracts under the Small Business Innovation Research Program and Small Business Technology Transfer Program.

PGI 227.7104-1 Policy.

See section 4(c) of the Small Business Administration's Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Program Policy Directive (effective May 3, 2023) for guidance on examples of SBIR/STTR phase III, which is available at https://www.sbir.gov/sites/default/files/SBA%20SBIR_STTR_POLICY_DIRECTIVE_May2023.pdf.

PGI 227.7104-2 Rights in SBIR or STTR data.

The clause under which the SBIR/STTR data were generated or developed will govern the Government's license rights in such SBIR/STTR data. The following examples illustratethe definition of the SBIR/STTR data protection period and the applicability of the DFARS 252.227-7018 clause:

(1) Redelivery of SBIR data.

(i) SBIR data first generated under a prior SBIR clause and redelivered under the current SBIR clause. In this example, a contractor generates and delivers SBIR data under a 2016 phase II SBIR contract that includes a prior version of the clause at DFARS 252.227-7018. The contractor delivers identical data in a contiguous series of follow-on contracts, including a later phase III contract that is an extension of the research effort in the 2016 contract. That phase III contract includes the current version of the clause at DFARS 252.227-7018. The contractor asserts SBIR data rights in these data. The 2016 contract included the clause at DFARS 252.227-7018, which defined the SBIR data protection period as the period commencing with contract award and ending upon the date 5 years after completion of the project from which such data were generated. This previous definition of the SBIR data protection period applies to the redelivered SBIR data in the contiguous series of follow-on contracts, including the later phase III contract. The SBIR data protection period is extended because the later contract derives from, extends, or completes an effort made under a prior SBIR contract that included the prior version of the clause at DFARS 252.227-7018. This is the case even under later contracts that include the current version of the clause at DFARS 252.227-7018 with a non-extendable 20-year SBIR/STTR data protection period. In addition, the SBIR data protection period from the prior version of the clause at DFARS 252.227-7018 may be extended indefinitely for subsequent redeliveries of identical SBIR data as long as the SBIR project has not been completed.

(ii) SBIR data first delivered with the 20-year SBIR data protection period and later redelivered under the current SBIR clause. In another example, a contractor generates and delivers SBIR data under a 2021 phase II SBIR contract. The contractor delivers identical data under a later phase III contract that is an extension of the research effort in the 2021 contract. The contractor asserts SBIR data rights in these data. That 2021 contract included a version of the DFARS 252.227-7018 clause that defines the SBIR data protection period as the period commencing on the date of contract award and ending 20 years after that date. The same definition of the SBIR/STTR data protection period applies to the redelivered SBIR data in the later phase III contract. Redelivery of identical SBIR data under any later contract will not extend the 20-year SBIR data protection period.

(2) Modifications to previously delivered SBIR or STTR data. A contractor generates and delivers SBIR/STTR data under a phase II STTR contract with the current version of the clause at DFARS 252.227-7018. The contractor develops and delivers modified STTR data under a later phase III contract. The contractor asserts SBIR/STTR data rights in these data. The previously delivered portions of the STTR data will be governed by the previous SBIR/STTR data protection period, while the newly developed portions of the STTR data will be governed by a new 20-year SBIR/STTR data protection period.

(3) SBIR or STTR data delivered under a contract and the contractor was not awarded a SBIR or STTR contract. A subcontractor was awarded a SBIR phase I contract. Later, the subcontractor performed SBIR phase III work under a contract awarded to a contractor who was not awarded a SBIR or STTR contract. The subcontractor furnished technical data and computer software deliverables related to SBIR phase III work performed under this contract. This technical data and computer software was furnished to the Government with SBIR data rights. The clause at DFARS 252.227-7018 should have been included either in the initial contract or via a contract modification, and the Government's rights in this SBIR data are subject to the terms of the clause at DFARS 252.227-7018.

PGI 227.72 - COMPUTER SOFTWARE, COMPUTER SOFTWARE DOCUMENTATION, AND ASSOCIATED RIGHTS

PGI 227.7200 Scope of subpart.

(b) The contracting officer should consider the following additional guidance and information regarding acquisition of computer software and computer software documentation:

(1) DoD Instruction 5000.74, Defense Acquisition of Services.

(2) DoD Instruction 5000.87, Operation of the Software Acquisition Pathway.

(3) DoD Instruction 5010.44, Intellectual Property (IP) Acquisition and Licensing.

PGI 227.7203 Other than commercial computer software and other than commercial computer software documentation.

PGI 227.7203-2 Acquisition of other than commercial computer software and computer software documentation and associated rights.

(b)(1) To the maximum extent practicable, an assessment of life-cycle needs should consider periodic delivery of computer software and computer software documentation including all executable code, source code, associated scripts, build procedures, automation scripts, tools, databases, libraries, test results, data sets, firmware, training materials, and any other elements necessary to integrate, test and evaluate, debug, deploy, and operate the software application in all relevant environments (e.g., development, staging, production). See DoDI 5010.44, Intellectual Property (IP) Acquisition and Licensing, sections 4.1 and 4.2, when formulating business advice and contract implementation strategies regarding the program manager's tailoring of software requirements to the needs of the Government.

(2)(i) *Procurement planning*.

(A) Based on the results of the assessment of life-cycle needs, and to the maximum extent practicable, the source code should be accompanied by all software capability descriptions (e.g., features, story points, use cases) and all as-built architecture and design products, traceability products, interface definitions including interfaces to proprietary software elements, and any other

requisite documentation.

(B) The assessment of life-cycle needs should consider delivery timelines to facilitate transition to a different contractor or to the Government. This approach facilitates management of program risk and supports options for flexibility in the transition of software sustainment to another organization.

(C) Contracting officers are responsible for ensuring that, wherever practicable, solicitations and contracts include the requirements for periodic delivery and any delivery timelines for computer software and computer software documentation, based upon the assessment of life-cycle needs.

(ii) *Alternatives to delivery of source code and related software design details.*

(A)(*1*)In determining whether the Government should require delivery of computer software source code and related software design details developed exclusively or partially at private expense, data managers and other requirements personnel are responsible for considering whether these alternatives permit the Government to—

(*ii*) Meet its management, engineering, and logistics needs; and

(*iii*) Maintain the currency of acquired technical data or software consistent with the assessment of life-cycle needs.

(*2*) To the extent practicable, the Government should also require open interface documentation for any privately developed computer software used in or interoperable with software developed for the Government, to allow for technology insertion on all sides of the interface, as applicable, and to support the use of modular open system approaches.

(B)Access agreements permit the Government to view, print, download, annotate, modify, or make derivatives of technical data or computer software stored within a contractor-controlled repository or facility (e.g., in an online environment or in person). Examples of access arrangements include remote online authorization to access an integrated data environment, product data management system operated by the contractor, or mechanisms authorizing physical entry to a contractor-controlled data repository, or cloud-based or subscription-based software products or services. The negotiated access agreement must stipulate permissions based on the assessment of life-cycle needs, and the access agreement must be made part of the contract.

(C) For each technical data or computer software requirement, the requiring activity must determine whether the Government’s needs can be better satisfied through access or formal delivery of the technical data or software (e.g., physical or electronic transfer of the data into Government custody). The Government should consider access to technical data or software when—

(*1*) The delivery of technical data or software is not cost-effective or feasible for technical, legal, or contractual reasons; and

(*2*) Access meets the Government’s needs for such technical data or software throughout the life-cycle of the program.

(D) Under a data escrow agreement, the Government and the contractor identify a third-party escrow agent that will keep designated technical data or computer software for safekeeping until a contractually specified condition occurs. If a contractually specified condition occurs, then the Government may obtain delivery of the escrowed technical data or computer software. The contracting officer shall include the data escrow agreement in the contract. The contract shall also include the Government’s license rights in the escrowed technical data or computer software. Use of

data escrow agreements is not preferable in all cases but may be useful when formal delivery or access is not feasible or cost-effective during the contract’s period of performance or delivery schedule.