

2018 REPORT
GOVERNMENT-INDUSTRY
ADVISORY PANEL ON
TECHNICAL DATA RIGHTS

NOVEMBER 13, 2018

TABLE OF CONTENTS

	Page
• Congressional Mandate	1
• Executive Summary of Findings & Recommendations	2-7
• Recommended Changes to <i>10 USC 2320 & 2321</i> Appendix A	8-19
• List of Advisory Panel Members Appendix B	20
• Tension Points Addressed Appendix C	21-25
• Tension Point White Papers Appendix D	26-27



Congressional Mandate

The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016 (Public Law 114-92), as amended in the FY2017 NDAA (Public Law 114-328), directed the Secretary of Defense to establish a Government-industry advisory panel (the Panel) for the purpose of reviewing Sections 2320 and 2321 of Title 10, United States Code (USC), regarding rights in technical data and the validation of proprietary data restrictions and the regulations implementing such sections, to ensure that such statutory and regulatory requirements are best structured to serve the interests of the taxpayers and the national defense.

Panel Membership

Government members of the Panel represented the office of the Secretary of Defense, the three military departments, and the legal, acquisition, logistics, and research and development communities in the Department of Defense. The private sector members of the Panel included independent experts and individuals representing the diversity of interested parties, including large and small businesses, traditional and non-traditional Government contractors, prime contractors and subcontractors, suppliers of hardware and software, and institutions of higher learning. A list of the Panel members appears in Appendix B.

Scope of Review

In conducting its review, the 813 Panel was charged with the following:

- (A) Ensure that the Department of Defense does not pay more than once for the same work.
- (B) Ensure that Department of Defense contractors are appropriately rewarded for their innovation and invention.
- (C) Provide for cost-effective re-procurement, sustainment, modification, and upgrades to Department of Defense systems.
- (D) Encourage the private sector to invest in new products, technologies, and processes relevant to the missions of the Department of Defense.
- (E) Ensure that the Department of Defense has appropriate access to innovative products, technologies, and processes developed by the private sector for commercial use.
- (F) Encourage the use of Modular Open System Architecture (MOSA).

Executive Summary

The Panel recognizes that the Department of Defense (DoD) and industry have different business models, which at times may be in conflict. In exploring common ground, the Panel members received the testimony of many defense and industry officials, reviewed the history of relevant legislation and identified “tension points” of disagreement between the Government and industry. Following extensive deliberations, Panel members (listed in Appendix B) prepared white papers to address the tension points and to make recommendations for legislative, regulatory, and policy changes that recognize and seek to balance the equities of both parties. In addition, the Panel identified several issues viewed as outside the purview of the Panel that were more appropriate to be considered by the FY 2016 NDAA, Section 809, Advisory Panel on Streamlining & Codifying Acquisition (the 809 Panel).

The Panel, as a whole, believes the topic of Intellectual Property (IP) (both rights and delivery requirements), while nuanced and complex, is a topic acquisition professionals must understand. Training, as recommended by the Panel, should help in this endeavor. Central to the issue is the fact that DoD does not always articulate its needs for upgrade and sustainment clearly enough and early enough in the system life cycle to allow industry to respond appropriately during the competitive and early planning stages. Some confuse IP delivery requirements with license rights. The Government’s (or any end user’s) license rights are of no value unless and until the data or software (e.g., IP deliverables) to which the license rights attach are requested and received. In addition, the training provided must address how the various federal organizations (e.g. Internal Revenue Service, the Federal Trade Commission, the Securities and Exchange Commission, and the International Trade Commission, the Federal Judiciary) and industry value IP. Best practices and standards in the field of IP valuation have been evolving over the past several decades among federal agencies, the courts, IP valuation specialty companies, and operating companies, and there is a body of literature reflecting these best practices and standards with which DoD acquisition professionals should be familiar. This will facilitate future negotiations and will help Government and industry reach a mutually acceptable position.

Tension Points

The Panel’s white papers to address tension points are categorized into eight broad areas: business model, acquisition planning and requirements, source selection and post source selection IP licensing, balancing the interests of the parties, implementation, compliance/administrative, data acquisition, and modular open systems approaches (MOSA). The Panel also identified several issues viewed as outside the purview of the Panel that were more appropriate to be considered by the 809 Panel. Appendix C is a spreadsheet that addresses the tension points, originally identified by the Panel, and their disposition.

1. Business Model: The Panel identified four separate tension points and consolidated them into one paper. The Panel does not believe legislative changes are required in this area but recommends the Government's long term requirements for sustainment and upgrade be included in solicitations early in the acquisition cycle, consider whether specially negotiated license rights (SNLR) are appropriate, and the impact of the Government's requirements on the potential for future competition (see Paper 1).

2. Acquisition Planning and Requirements: The Panel identified eight separate tension points, but in its final deliberation, wrote two papers and consolidated the others into papers in other areas of the report. The Panel does not believe legislative changes are needed in this area. One paper deals with access to information where a contract-required data requirement (Contract Data Requirements List (CDRL)) is either inappropriate or may not be possible (e.g., cyber security breach reviews). The other deals with streamlining data requirements for research contracts using Budget Authority 6.1 and 6.2 funds (see Papers 2 and 3).

3. Source Selection and Post Source Selection IP Licensing: The Panel identified four separate tension points and consolidated them into three papers. One deals with evaluating IP during source selection. The Panel was provided a variety of examples used in source selections and their impacts; some good, some bad. The Panel agreed the Government should create regulations reflecting specific principles to increase transparency and to ensure IP is properly valued when used as an evaluation factor without mandating offerors to relinquish their IP. Because of the wide range of major weapon system requirements, the Panel was unable to coalesce on a single method and recommends a pilot program for IP evaluation in acquisition planning and source selection (see Paper 4). The second paper deals with the treatment of special clauses developed to implement IP strategies. The Panel recommends the Cadre of IP Experts required by 10 USC 2322 be tasked to clarify the use of these clauses (see Paper 6). The third paper deals with IP valuation. The panel discussed challenges with determining how to negotiate a fair and reasonable price for IP rights, such as in situations where the Government seeks to acquire greater IP rights, or additional IP deliverables, than is customarily provided in the commercial marketplace. The panel recommends the use of broadly accepted best practices, norms, and standards in IP valuation by both the Government and industry (see Paper 5).

4. Balancing the Interests of the Parties: The Panel identified nine separate tension points and consolidated them into six papers divided into two sets. The first set addressed how development is funded. The Panel recommends retaining the current source of funding policy (see Paper 8), but was unable to reach agreement on how independent research and development (IR&D) and other indirect costs should be treated for purposes of determining the Government's IP rights and recommends further study (see Paper 7). The final paper of this set deals with modifications made to commercial items to meet Government unique needs and the Panel recommends several changes to the Defense Federal Acquisition Regulation Supplement (DFARS) to clarify how the issue should be addressed (see Paper 9). The second set addresses data rights in relation to needs. One paper deals with changes to policy required to align commercial license requirements

with Government needs (see Paper 10). Another recommends a statutory change to limit segregation or reintegration data to the end item level or higher (see Paper 11). The last paper addresses the form of data and data rights necessary to fulfill maintenance and sustainment requirements for equipment and software and expressly recommends software maintenance be defined (see Paper 12).

5. Implementation: The Panel identified 12 separate issues and consolidated them into seven papers. In two papers there was a disagreement among Panel members and minority positions were prepared (see Papers 14 and 19). One paper deals with technical data and computer software and recommends that the differences be clearly defined in regulation (see Paper 13). The next paper deals with development versus adaptation and is related to the source of funding discussion above (see Paper 14 and minority position). Another paper deals with data necessary for operation, maintenance, installation, or training (OMIT), and the exclusion of detailed manufacturing or process data (DMPD) from the definition of OMIT data, and recommends clearer definitions in policy (see Paper 15). One paper encourages the use of SNLRs when appropriate (see Paper 16). One paper recommends DoD create standard data definitions for specific data categories tied to unlimited rights, such as form fit function (FFF), OMIT (excluding DMPD), computer software documentation, and other categories (see Paper 17). One paper deals with the validation process required by 10 USC 2321 and recommends a statutory change to simplify and clarify how validation is accomplished and challenged for both contractors and subcontractors (see Paper 18). The final paper recommends changes to the mandatory flow down of clauses to commercial subcontractors and suppliers (see Paper 19 and minority position).

6. Compliance/Administrative: The Panel identified four separate issues. They involve CDRLs, Small Business Innovation Research (SBIR), training and data assertion lists. One paper recommends policy changes to address mechanisms to keep data current throughout the life cycle of a system (see Paper 20). The second recommends a statutory change to make clear that when SBIR regulations apply, the development will be treated, during the SBIR data rights protection period, as if it were developed at private expense (see Paper 21). The third deals with the lack of trained personnel and recommends training for the acquisition workforce and the creation of a cadre of subject matter experts. The Panel notes that the 2018 NDAA adopted the Panel's recommendation and required the creation of such a cadre at 10 USC 2322 (see Paper 22). The final paper recommends several regulatory changes to simplify and clarify the requirements for data assertion during source selection and contract execution (see Paper 23).

7. Data Acquisition: The Panel identified six separate issues and consolidated them into five papers. In one paper there was a disagreement among the members and a minority position paper was provided (see Paper 24). The first paper deals with deferred ordering. The Panel recommended a statutory change that would allow the Government to exempt, at their discretion, data from deferred ordering, which is consistent with the current regulation. The minority position recommends the Government follow the 10 USC 2320 as it stands (albeit unimplemented), without changes, in regard to deferred ordering (see Paper 24 and minority paper). The next paper recommends a statutory change to extend the time period for priced options for delivery of data rights (see Paper 25). Another paper recommends regulatory changes

to make clear the limits of deferred ordering in the context of interface data (see Paper 26). One paper recommends regulatory changes that should improve the early identification of required data and thus reduce the need for deferred ordering of data (see Paper 27). The final paper recommends regulatory changes to discuss escrow agreements that would reduce the need for deferred ordering (see Paper 28).

8. Modular Open Systems Approaches (MOSA): The Panel identified three separate issues and consolidated them into two papers. The first deals with GPR in major system interfaces and makes several regulatory recommendations that should clarify the statutory intent, and therefore reduce execution risk (see Paper 29). The second deals with GPR in interfaces (other than major system interfaces) developed with mixed funding and makes a statutory recommendation to clarify the intent of the legislation (see Paper 30).

9. The 809 Panel: Members of the 813 Panel met with the 809 Panel and shared eight areas where the 813 Panel believed it would be more appropriate for the 809 Panel to make recommendations based on their charter (see below).

Appendix A is the line-in/line-out of 10 USC 2320 and 2321 recommended by the Panel. Each recommendation for change is linked to a paper (Appendix D).

The eight papers with recommendations for statutory changes to 10 USC 2320 and 2321 are:

- 1) Authorized release and use of limited rights technical data (Paper 11) (10 USC 2320)
- 2) Development versus Adaptation (Paper 14a) (10 USC 2320 & 2321) with Minority report (Paper 14b)
- 3) The Validation Process is Cumbersome and Confusing (Paper 18a) (10 USC 2321) and line-in/line-out (Paper 18b)
- 4) Mandatory flow-down (commercial subs and suppliers) (Paper 19a) with Minority report (Paper 19b) (10 USC 2320 & 2321)
- 5) Small Business Innovation Research (SBIR) (Flow-down to Suppliers; Inability to Share with Primes; Evaluation) (Paper 21) (10 USC 2320)
- 6) Deferred ordering period: 6 years (rather than perpetual) and Deferred Ordering Part 1: only data “generated” under the contract (Paper 24a) (10 USC 2320) with Minority Report (Paper 24b)
- 7) Time Limits on Priced Contract Options (Paper 25) (10 USC 2320)
- 8) GPR in Interfaces Developed with Mixed Funding (Paper 30) (10 USC 2320)

Three papers have recommendations for statute other than 10 USC 2320 and 2321. They are:

- 1) Lack of Trained Personnel (Paper 22) (partially implemented in the FY2018 NDAA)
- 2) Data Rights as an Evaluation Factor (Paper 4)

- 3) Treatment of Independent Research and Development (IR&D) versus Self-Funded Research and Development (SFR&D) for Intellectual Property (IP) rights determinations; IR&D risk correct for limited/restricted rights? (Paper 7)

The remaining papers make recommendations for changes to policy or regulation that do not require statutory change. Of note, the Defense Acquisition Regulation Council (DARC) agreed during the Panel's deliberations that, as an exception to their normal process, industry would be invited to participate in the rule making using public meetings. Industry will be invited to participate in the actual drafting of the rule and the adjudication of the comments received from the public.

The 19 recommendations for changes to policy or regulation are:

- 1) Different Business Models in Government and Industry result in different objectives (Paper 1)
- 2) Access for limited purposes (cyber review; airworthiness; approvals) versus delivery as a Contract Data Requirements List (CDRL) (Paper 2)
- 3) Contract Data Requirements List (CDRL) requirements for Budget Activities 6.1 and 6.2 Research Programs versus CDRL requirements for Production/Sustainment (Paper 3)
- 4) Intellectual Property (IP) Valuation (Paper 5)
- 5) Contract Requirements in Section H Should not be treated like Standard Clauses (Paper 6)
- 6) Is Source of Funding the Best Way to Determine Rights to Technical Data? (Paper 8)
- 7) Commercial vs. Noncommercial Items (Paper 9)
- 8) Commercial Software License versus Government-unique Requirements (Paper 10)
- 9) Are existing rights sufficient for maintenance and sustainment? (Paper 12)
- 10) Software versus Technical Data (Paper 13)
- 11) Operation, Maintenance, Installation, and Training (OMIT) Data versus Detailed Manufacturing or Process Data (DMPD), including such data pertaining to a major system component (Paper 15)
- 12) Rigid Intellectual Property (IP) requirements versus Flexible Arrangements (Paper 16)
- 13) Poor Data Item Description (DID) Alignment with Statutory/regulatory Categories Form, Fit and Function (FFF) and Operation, Maintenance, Installation or Training (OMIT) (Paper 17)
- 14) How to keep CDRL deliverable up-to-date (Paper 20)
- 15) The Data Assertion List is a Burden on Both Contractor and the Government (Paper 23)
- 16) Deferred Ordering Part 2: all interface or major systems interface data may be ordered regardless of U.S. Government development (Paper 26)

- 17) Failure to Define and Order CDRLs (Reliance on Deferred Ordering and DAL to Obtain Data (Paper 27)
- 18) Escrow as a Form of Deferred Delivery (Paper 28)
- 19) Government Purpose Rights (GPR) in Major System Interface (MSI) (Developed Exclusively at Private Expense (DEPE) or with Mixed Funding) (Paper 29)

The topics discussed with the 809 Panel were:

- 1) Poor alignment between 10 USC 2320 and other marking clauses (distribution statements in DFARS 252.204-7000) and contract attachments such as DIDs and the DAL
- 2) Complexity of the IP scheme versus the ability of commercial and small business to comply.
- 3) Synchronization of sustainment policies and data rights. (10 USC 2460 vs 2320)
- 4) Maintaining currency in training certifications.
- 5) Strategy and plans development; who should be engaged? Who is engaged?
- 6) Multiple definitions of commercial item in statute.
- 7) Applicability of flow down in clauses.
- 8) No definition of subcontractor versus supplier.

Conclusion

The above are, in the Panel's opinion, the major issues addressed.

Government and industry recognize that they have differing positions on certain IP issues. However, they are united regarding the important contributions of both parties to ensure that our Nation's warriors are equipped with state of the art equipment to defend the nation. DoD recognizes that private industry plays a vital role in ensuring that innovative technologies continue to be developed to support the ever changing needs of the warfighter. Industry recognizes that DoD must ensure that support of the Warfighter is accomplished in a cost-effective way while protecting the interests of the taxpayer.

10 USC 2320 - Rights in technical data

(a)(1) The Secretary of Defense shall prescribe regulations to define the legitimate interest of the United States and of a contractor or subcontractor in technical data pertaining to an item or process. Such regulations shall be included in regulations of the Department of Defense prescribed as part of the Federal Acquisition Regulation. Such regulations may not impair any right of the United States or of any contractor or subcontractor with respect to patents or copyrights or any other right in technical data otherwise established by law. Such regulations also may not impair the right of a contractor or subcontractor to receive from a third party a fee or royalty for the use of technical data pertaining to an item or process developed exclusively at private expense by the contractor or subcontractor, except as otherwise specifically provided by law.

(2) Such regulations shall include the following provisions:

(A) Development exclusively with federal funds.

(i) Except as provided in subparagraph (ii), in the case of an item or process that is developed by a contractor or subcontractor exclusively with Federal funds (other than an item or process developed under a contract or subcontract to which regulations under section 9(j)(2) of the Small Business Act (15 U.S.C. 638(j)(2)) apply), the United States shall have the unlimited right to-

(iI) use technical data pertaining to the item or process; or
(iiI) release or disclose the technical data to persons outside the government or permit the use of the technical data by such persons.

(ii) Small business innovation research. An item or process developed under a contract or subcontract to which regulations under section 9(j)(2) of the Small Business Act (15 U.S.C. 638(j)(2)) apply shall be treated as an item or process developed at private expense, except as otherwise permitted by those regulations. Upon the expiration of the protection period authorized in those regulations, the rights of the United States shall be as set forth in subparagraph (i).¹

(B) Development exclusively at private expense.-Except as provided in subparagraphs (C), (D), and (G), in the case of an item or process that is developed by a contractor or subcontractor exclusively at private expense, the contractor or subcontractor may restrict the right of the United States to release or disclose technical data pertaining to the item or process to persons outside the government or permit the use of the technical data by such persons.

(C) Exception to subparagraph (b).-Subparagraph (B) does not apply to technical data that-

¹ Change recommended in SBIR – flow down to suppliers; inability to share with primes; how evaluated (Paper 21).

- (i) constitutes a correction or change to data furnished by the United States;
- (ii) relates to form, fit, or function;
- (iii) is necessary for operation, maintenance, installation, or training (other than detailed manufacturing or process data, including such data pertaining to a major system component); or
- (iv) is otherwise publicly available or has been released or disclosed by the contractor or subcontractor without restriction on further release or disclosure.

(D) Exception to subparagraph (b).-Notwithstanding subparagraph (B), the United States may release or disclose technical data to persons outside the Government, or permit the use of technical data by such persons, if-

- (i) such release, disclosure, or use-
 - (I) is necessary for emergency repair and overhaul;
 - (II) is a release, disclosure, or use of technical data pertaining to the an interface between an item or process and other items or processes necessary for the segregation of the 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;² or
 - (III) is a release or disclosure of technical data (other than detailed manufacturing or process data) to, or use of such data by, a foreign government that is in the interest of the United States and is required for evaluational or informational purposes;
- (ii) such release, disclosure, or use is made subject to a prohibition that the person to whom the data is released or disclosed may not further release, disclose, or use such data; and
- (iii) the contractor or subcontractor asserting the restriction is notified of such release, disclosure, or use.

(E) Development with mixed funding.-Except as provided in subparagraphs (F) and (G), in the case of an item or process that is developed in part with Federal funds and in part at private expense, the respective rights of the United States and of the contractor or subcontractor in technical data pertaining to such item or process shall be established as early in the acquisition process as practicable (preferably during contract negotiations) and shall be based on negotiations between the United States and the contractor, except in any case in which the Secretary of Defense determines, on the basis of criteria established in the regulations, that negotiations would not be

² Change recommended in Authorized release and use of limited rights technical data (Paper 11).

practicable. The establishment of such rights shall be based upon consideration of all of the following factors:

- (i) The statement of congressional policy and objectives in section 200 of title 35, the statement of purposes in section 2(b) of the Small Business Innovation Development Act of 1982 (15 U.S.C. 638 note), and the declaration of policy in section 2 of the Small Business Act (15 U.S.C. 631).
- (ii) The interest of the United States in increasing competition and lowering costs by developing and locating alternative sources of supply and manufacture.
- (iii) The interest of the United States in encouraging contractors to develop at private expense items for use by the Government.
- (iv) Such other factors as the Secretary of Defense may prescribe.

(F) Interfaces developed with mixed funding.-Notwithstanding subparagraph (E), the United States shall have government purpose rights in technical data pertaining to an interface (between interface between an item or process and other items or processes) that processes that was developed in part with Federal funds and in part at private expense³, except in any case in which the Secretary of Defense determines, on the basis of criteria established in the regulations, that negotiation of different rights in such technical data would be in the best interest of the United States.

(G) Major system interfaces developed exclusively at private expense or with mixed funding.- Notwithstanding subparagraphs (B) and (E), the United States shall have government purpose rights in technical data pertaining to a major system interface developed exclusively at private expense or in part with Federal funds and in part at private expense and used in a modular open system approach pursuant to section 2446a of this title, except in any case in which the Secretary of Defense determines that negotiation of different rights in such technical data would be in the best interest of the United States. Such major system interface shall be identified in the contract solicitation and the contract. For technical data pertaining to a major system interface developed exclusively at private expense for which the United States asserts government purpose rights, the Secretary of Defense shall negotiate with the contractor the appropriate and reasonable compensation for such technical data.

(H) A contractor or subcontractor (or a prospective contractor or subcontractor) may not be required, as a condition of being responsive to a solicitation or as a condition for the award of a contract-

- (i) to sell or otherwise relinquish to the United States any rights in technical data except-

³ Change recommended in GPR in interfaces developed with mixed funding (Paper 30).

- (I) rights in technical data described in subparagraph (A) for which a use or release restriction has been erroneously asserted by a contractor or subcontractor;
 - (II) rights in technical data described in subparagraph (C); or
 - (III) under the conditions described in subparagraph (D); or
- (ii) to refrain from offering to use, or from using, an item or process to which the contractor is entitled to restrict rights in data under subparagraph (B).

- (I) The Secretary of Defense may-
 - (i) negotiate and enter into a contract with a contractor or subcontractor for the acquisition of rights in technical data not otherwise provided under subparagraph (C) or (D), if necessary to develop alternative sources of supply and manufacture;
 - (ii) agree to restrict rights in technical data otherwise accorded to the United States under this section if the United States receives a royalty-free license to use, release, or disclose the data for purposes of the United States (including purposes of competitive procurement); or
 - (iii) permit a contractor or subcontractor to license directly to a third party the use of technical data which the contractor is otherwise allowed to restrict, if necessary to develop alternative sources of supply and manufacture.

(J) Notwithstanding subparagraphs (A) through (G), in the case of a commercially available off-the-shelf item, as defined in section 104 of title 41—

- (i) the United States shall acquire only the technical data, and the rights in such technical data, that are customarily provided to the public, unless such technical data or rights are inconsistent with federal law or do not satisfy the needs of the United States; and
- (ii) the Secretary of Defense shall negotiate with the contractor or subcontractor for any additional technical data or rights necessary to satisfy the needs of the United States.⁴

- (3) The Secretary of Defense shall define the terms "developed", "exclusively with Federal funds", and "exclusively at private expense" in regulations prescribed under paragraph (1). In defining such terms, the Secretary shall specify the manner in which indirect costs shall be treated and shall specify that amounts spent for independent research and development and bid and proposal costs shall not be considered to be Federal funds for the purposes of the definitions under this paragraph.

⁴ Change recommended in Mandatory flow-down (commercial subs and suppliers) (Paper 19a, majority position). *Compare*, minority position reflected in Paper 19b.

(b) Regulations prescribed under subsection (a) shall require that, whenever practicable, a contract for supplies or services entered into by an agency named in section 2303 of this title contain appropriate provisions relating to technical data, including provisions-

- (1) defining the respective rights of the United States and the contractor or subcontractor (at any tier) regarding any technical data to be delivered under the contract and providing that, in the case of a contract for a commercial item, the item shall be presumed to be developed at private expense unless shown otherwise in accordance with section 2321(f);
- (2) specifying the technical data, if any, to be delivered under the contract and delivery schedules for such delivery;
- (3) establishing or referencing procedures for determining the acceptability of technical data to be delivered under the contract;
- (4) establishing separate contract line items for the technical data, if any, to be delivered under the contract;
- (5) to the maximum practicable extent, identifying, in advance of delivery, technical data which is to be delivered with restrictions on the right of the United States to use such data;
- (6) requiring the contractor to revise any technical data delivered under the contract to reflect engineering design changes made during the performance of the contract and affecting the form, fit, and function of the items specified in the contract and to deliver such revised technical data to an agency within a time specified in the contract;
- (7) establishing remedies to be available to the United States when technical data required to be delivered or made available under the contract is found to be incomplete or inadequate or to not satisfy the requirements of the contract concerning technical data;
- (8) authorizing the head of the agency to withhold payments under the contract (or exercise such other remedies as the head of the agency considers appropriate) during any period if the contractor does not meet the requirements of the contract pertaining to the delivery of technical data;
- (9) providing that, in addition to technical data that is already subject to a contract delivery requirement, and except for data (other than data described at paragraphs (A) and (G) of subsection (a)(2)) that the government and the contractor have agreed will not be subject to deferred ordering,⁵ the United States may require, until the date occurring six years after acceptance of the last item (other than technical data) under a contract or the date of contract termination, whichever is later, the delivery of technical data that has been generated in the performance of the contract, and compensate the contractor only for reasonable costs incurred for having converted and delivered the data in the required form, upon a determination that-

⁵ Change recommended in Deferred ordering period: 6 years (rather than perpetual) and Deferred Ordering Part 1: only data “generated” under the contract (Paper 24a, majority position). *Compare*, minority position reflected in Paper 24b.

(A) the technical data is needed for the purpose of reprocurement, sustainment, modification, or upgrade (including through competitive means) of a major system or subsystem thereof, a weapon system or subsystem thereof, or any noncommercial item or process; and

(B) the technical data-

(i) pertains to an item or process developed in whole or in part with Federal funds; or

(ii) is described in subparagraphs (D)(i)(II), (F), and (G) of subsection (a)(2); and

(10) providing that the United States is not foreclosed from requiring the delivery of the technical data by a failure to challenge, in accordance with the requirements of section 2321(d) of this title, the contractor's assertion of a use or release restriction on the technical data.

(c) Nothing in this section or in section 2305(d) of this title prohibits the Secretary of Defense from-

(1) prescribing standards for determining whether a contract entered into by the Department of Defense shall provide for a time to be specified in the contract after which the United States shall have the right to use (or have used) for any purpose of the United States all technical data required to be delivered to the United States under the contract or providing for such a period of time (not to exceed 7 years) as a negotiation objective;

(2) notwithstanding any limitation upon the license rights conveyed under subsection (a), allowing a covered Government support contractor access to and use of any technical data delivered under a contract for the sole purpose of furnishing independent and impartial advice or technical assistance directly to the Government in support of the Government's management and oversight of the program or effort to which such technical data relates; or

(3) prescribing reasonable and flexible guidelines, including negotiation objectives, for the conduct of negotiations regarding the respective rights in technical data of the United States and the contractor.

(d) The Secretary of Defense shall by regulation establish programs which provide domestic business concerns an opportunity to purchase or borrow replenishment parts from the United States for the purpose of design replication or modification, to be used by such concerns in the submission of subsequent offers to sell the same or like parts to the United States. Nothing in this subsection limits the authority of the head of an agency to impose restrictions on such a program related to national security considerations, inventory needs of the United States, the improbability of future purchases of the same or like parts, or any additional restriction otherwise required by law.

(e) The Secretary of Defense shall require program managers for major weapon systems and subsystems of major weapon systems to assess the long-term technical data needs of such systems and subsystems and establish corresponding acquisition strategies that provide for technical data rights needed to sustain such systems and subsystems over their life cycle. Such strategies may include the development of maintenance capabilities within the Department of Defense or competition for contracts for sustainment of such systems

or subsystems. Assessments and corresponding acquisition strategies developed under this section with respect to a weapon system or subsystem shall-

- (1) be developed before issuance of a contract solicitation for the weapon system or subsystem;
- (2) to the extent practicable, require the use of appropriate contract mechanisms (e.g., address the merits of including a priced contract options, not to exceed 20 years; escrow arrangements) for the future delivery of technical data and associated license rights that were not acquired upon initial contract award but may be necessary to support the life cycle sustainment plan;⁶
- (3) address the potential for changes in the sustainment plan over the life cycle of the weapon system or subsystem; and
- (4) apply to weapon systems and subsystems that are to be supported by performance-based logistics arrangements as well as to weapons systems and subsystems that are to be supported by other sustainment approaches.

(f) Preference for Specially Negotiated Licenses.-The Secretary of Defense shall, to the maximum extent practicable, negotiate and enter into a contract with a contractor for a specially negotiated license for technical data to support the product support strategy of a major weapon system or subsystem of a major weapon system. In performing the assessment and developing the corresponding strategy required under subsection (e) for such a system or subsystem, a program manager shall consider the use of specially negotiated licenses to acquire customized technical data appropriate for the particular elements of the product support strategy.

(g) Covered Government Support Contractor Defined.-In this section, the term "covered Government support contractor" means a contractor under a contract the primary purpose of which is to furnish independent and impartial advice or technical assistance directly to the Government in support of the Government's management and oversight of a program or effort (rather than to directly furnish an end item or service to accomplish a program or effort), which contractor-

- (1) is not affiliated with the prime contractor or a first-tier subcontractor on the program or effort, or with any direct competitor of such prime contractor or any such first-tier subcontractor in furnishing end items or services of the type developed or produced on the program or effort; and
- (2) executes a contract with the Government agreeing to and acknowledging-

- (A) that proprietary or nonpublic technical data furnished will be accessed and used only for the purposes stated in that contract;
- (B) that the covered Government support contractor will enter into a non-disclosure agreement with the contractor to whom the rights to the technical data belong;

⁶ Change recommended in Time Limits on Priced Contract Options (Paper 25).

- (C) that the covered Government support contractor will take all reasonable steps to protect the proprietary and nonpublic nature of the technical data furnished to the covered Government support contractor during the program or effort for the period of time in which the Government is restricted from disclosing the technical data outside of the Government;
 - (D) that a breach of that contract by the covered Government support contractor with regard to a third party's ownership or rights in such technical data may subject the covered Government support contractor
 - (i) to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and
 - (ii) to civil actions for damages and other appropriate remedies by the contractor or subcontractor whose technical data is affected by the breach; and
 - (E) that such technical data provided to the covered Government support contractor under the authority of this section shall not be used by the covered Government support contractor to compete against the third party for Government or non-Government contracts.
- (h) Additional Definitions.-In this section, the terms "major system component", "major system interface", and "modular open system approach" have the meanings provided in section 2446a of this title.

10 USC 2321 - Validation of proprietary data restrictions

- (a) Contracts Covered by Section.-This section applies to any contract for supplies or services (except for commercially available off-the-shelf items, as defined in section 104 of Title 41) entered into by the Department of Defense that includes provisions for the delivery of technical data or noncommercial computer software⁷. In the case of all other commercial items, this section shall apply except to the extent specified in the contract in accordance with criteria specified by the Secretary to balance the respective interests of the United States and the contractor or subcontractor.⁸
- (b) Contractor Justification for Restrictions.-A contract subject to this section shall provide that a contractor under the contract and any subcontractor under the contract at any tier shall be prepared to furnish to the contracting officer a written justification for any use or release restriction (as defined in subsection (i)) asserted by the contractor or subcontractor.

⁷ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

⁸ Change recommended in Development versus Adaptation (Paper 14a, majority position) and Mandatory flow-down (commercial subs and suppliers) (Paper 19a, majority position). *Compare*, minority positions reflected in Papers 14b and 19b, respectively.

(c) Review of Restrictions.-(1) The Secretary of Defense shall ensure that there is a thorough review of the appropriateness of any use or release restriction asserted with respect to technical data or noncommercial computer software⁹ by a contractor or subcontractor at any tier under a contract subject to this section.

(2) The review of an asserted use or release restriction under paragraph (1) shall be conducted before the end of the three-year period beginning on the later of-

(A) the date on which final payment is made on the contract under which the technical data or noncommercial computer software¹⁰ is required to be delivered; or

(B) the date on which the technical data or noncommercial computer software¹¹ is delivered under the contract.

(d) Challenges to Restrictions.-(1) The Secretary of Defense may challenge a use or release restriction asserted with respect to technical data or noncommercial computer software¹² by a contractor or subcontractor at any tier under a contract subject to this section if the Secretary finds that-

(A) reasonable grounds exist to question the current validity of the asserted restriction; and

(B) the continued adherence by the United States to the asserted restriction would make it impracticable to procure the item to which the technical data pertain or noncommercial computer software¹³ competitively at a later time.

(2)(A) A challenge to a use or release restriction asserted by the contractor in accordance with applicable regulations may not be made under paragraph (1) after the end of the six-year period described in subparagraph (B) unless the technical data or noncommercial computer software¹⁴ involved-

(i) are publicly available;

(ii) have been furnished to the United States without restriction;

(iii) have been otherwise made available without restriction; or

(iv) are the subject of a fraudulently asserted use or release restriction.

(B) The six-year period referred to in subparagraph (A) is the six-year period beginning on the later of-

⁹ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

¹⁰ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

¹¹ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

¹² Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

¹³ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

¹⁴ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

(i) the date on which the final item payment (other than technical data or noncommercial computer software) is accepted made on the contract under which the technical data or noncommercial computer software¹⁵ are required to be delivered; or

(ii) the date on which the technical data or noncommercial computer software¹⁶ are delivered under the contract.

(3) If the Secretary challenges an asserted use or release restriction under paragraph (1), the Secretary shall provide written notice of the challenge to the contractor or subcontractor asserting the restriction. Any such notice shall-

- (A) state the specific grounds for challenging the asserted restriction;
- (B) require a response within 60 days justifying the current validity of the asserted restriction; and
- (C) state that evidence of a justification described in paragraph (4) may be submitted.

(4) It is a justification of an asserted use or release restriction challenged under paragraph (1) that, within the three-year period preceding the challenge to the restriction, the Department of Defense validated a restriction identical to the asserted restriction if-

- (A) such validation occurred after a challenge to the validated restriction under this subsection; and
- (B) the validated restriction was asserted by the same contractor or subcontractor (or a licensee of such contractor or subcontractor).

(e) Time for Contractors to Submit Justifications.-If a contractor or subcontractor asserting a use or release restriction submits to the contracting officer a written request, showing the need for additional time to comply with the requirement to justify the current validity of the asserted restriction, additional time to adequately permit the submission of such justification shall be provided by the contracting officer as appropriate. If a party asserting a restriction receives notices of challenges to restrictions on technical data or noncommercial computer software¹⁷ from more than one contracting officer, and notifies each contracting officer of the existence of more than one challenge, the contracting officer initiating the first in time challenge, after consultation with the party asserting the restriction and the other contracting officers, shall formulate a schedule of responses to each of the challenges that will afford the party asserting the restriction with an equitable opportunity to respond to each such challenge.

(f) Presumption of Development Exclusively at Private Expense.-(1) Except as provided in paragraph (2), in In the case of a challenge to a use or release restriction that is asserted with respect to technical data of a contractor or subcontractor under a contract for commercial items, the contracting officer shall presume that the contractor or subcontractor has justified the restriction on the basis that the item was developed exclusively at private expense, whether or not the contractor or subcontractor submits a justification in

¹⁵ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

¹⁶ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

¹⁷ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

response to the notice provided pursuant to subsection (d)(3).¹⁸ In such a case, the challenge to the use or release restriction may be sustained only if information provided by the Department of Defense demonstrates that the item was not developed exclusively at private expense.

(2) ~~In the case of a challenge to a use or release restriction that is asserted with respect to technical data of a contractor or subcontractor for a major system or a subsystem or component thereof on the basis that the major weapon system, subsystem, or component was developed exclusively at private expense-~~

~~(A) the presumption in paragraph (1) shall apply-~~

~~(i) with regard to a commercial subsystem or component of a major system, if the major system was acquired as a commercial item in accordance with section 2379(a) of this title;~~

~~(ii) with regard to a component of a subsystem, if the subsystem was acquired as a commercial item in accordance with section 2379(b) of this title; and~~

~~(iii) with regard to any other component, if the component is a commercially available off-the-shelf item or a commercially available off-the-shelf item with modifications of a type customarily available in the commercial marketplace or minor modifications made to meet Federal Government requirements; and~~

~~(B) in all other cases, the challenge to the use or release restriction shall be sustained unless information provided by the contractor or subcontractor demonstrates that the item was developed exclusively at private expense.¹⁹~~

(g) Decision by Contracting Officer.-
(1) Upon a failure by the contractor or subcontractor to submit any response under subsection (d)(3), the contracting officer shall issue a decision pertaining to the validity of the asserted restriction.

(2) After review of any justification submitted in response to the notice provided pursuant to subsection (d)(3), the contracting officer shall, within 60 days of receipt of any justification submitted, issue a decision or notify the party asserting the restriction of the time within which a decision will be issued.

(h) Claims. —

~~If a claim pertaining to the validity of the asserted restriction is submitted in writing to a contracting officer by a contractor or subcontractor at any tier, such claim shall be considered a claim within the meaning of chapter 71 of title 41. Any appeal by a contractor or subcontractor of a decision under (g) shall be considered a claim within the meaning of chapter 71 of title 41, and the contractor or subcontractor~~

¹⁸ Change recommended in Mandatory flow-down (commercial subs and suppliers) (Paper 19).

¹⁹ Change recommended in Mandatory flow-down (commercial subs and suppliers) (Paper 19). Note, this revision has already been made by Section 865 of the FY2019 NDAA (Pub.L. 115-232).

asserting the restriction which is the subject of the decision under (g) shall be considered a "contractor" within the meaning of chapter 71 of title 41.²⁰

(i) Rights and Liability Upon Final Disposition.-
(1) If, upon final disposition, the contracting officer's challenge to the use or release restriction is sustained-

(A) the restriction shall be cancelled; and

(B) if the asserted restriction is found not to be substantially justified, the contractor or subcontractor asserting the restriction shall be liable to the United States for payment of the cost to the United States of reviewing the asserted restriction and the fees and other expenses (as defined in section 2412(d)(2)(A) of title 28) incurred by the United States in challenging the asserted restriction, unless special circumstances would make such payment unjust.

(2) If, upon final disposition, the contracting officer's challenge to the use or release restriction is not sustained-

(A) the United States shall continue to be bound by the restriction; and

(B) the United States shall be liable for payment to the party asserting the restriction for fees and other expenses (as defined in section 2412(d)(2)(A) of title 28) incurred by the party asserting the restriction in defending the asserted restriction if the challenge by the United States is found not to be made in good faith.

(j) Use or Release Restriction Defined.-In this section, the term "use or release restriction", with respect to technical data or noncommercial computer software²¹ delivered to the United States under a contract subject to this section, means a restriction by the contractor or subcontractor on the right of the United States-

(1) to use such technical data or noncommercial computer software²²; or

(2) to release or disclose such technical data or noncommercial computer software²³ to persons outside the Government or permit the use of such technical data or noncommercial computer software²⁴ by persons outside the Government.

²⁰ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

²¹ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

²² Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

²³ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

²⁴ Change recommended in The Validation Process is Too Cumbersome and Confusing for Use (Paper 18).

APPENDIX B

GOVERNMENT-INDUSTRY ADVISORY PANEL MEMBERS

1. Ms. Kelly D. Alexander, U.S. Army *
2. Mr. Elliot B. Branch, U.S. Navy
3. Dr. Alison K. Brown, Ph.D.
4. Mr. Thomas P. Dee, U.S. Navy*
5. Mr. Bill Elkington, Rockwell Collins
6. Rear Admiral (Lower Half) Richard T. Ginman, Supply Corps, U.S. Navy (Ret.) - Chairman
7. Mr. Joseph Gordon, U.S. Air Force
8. Mr. Richard M. Gray, J.D., OSD
9. Dr. Roger D. Hamerlinck, D.B.A., U.S. Army
10. Lt. Colonel Theodora S. Hancock, U.S. Air Force (Ret.) & SAF/AQ
11. Mr. Charles H. Harris, J.D., U.S. Army
12. Ms. Kelly Kyes, J.D., The Boeing Company
13. Mr. James McEwen, J.D., Sikorsky, a Lockheed Martin Company
14. Mr. Sean O'Brien, J.D., United Technologies Corporation
15. Mr. Carl D. Rapp, Vice President, Timken
16. Mr. Charles A. Thomasian, J.D. **

* Limited participation due to reassignment

** Did not participate

APPENDIX C

Statutory						
Paper Number	Tension Point	2320	2321	Other	Regulatory	Notes
1. Business model concerns.						
1	a. Difference in business plans between Government and industry.	No	No	No	Yes	Paper complete Includes 1b, c, d, 2a, 4biii
	b. Commercial return on investment over years versus depot and competition requirements.					Moved into 1a
	c. For-profit model versus non-profit business model conflict.					Moved into 1a
	d. Government as customer versus Government as competitor (depot; labs).					Moved into 1a
2. Acquisition planning and requirements.						
	a. GPR: Scope, sunset, one size does not fit all paths to competition.					Moved into 1a
	b. Depot-level maintenance capability/requirements.					moved into 4biv.
	c. Sustainment is more than maintenance					moved into 4biv.
	d. What is necessary to comply with 2320(e)(3)'s requirement to address TD (and CS) needs in view of potential changes to sustainment strategy.					moved into 4biv
2	e. Access for limited purposes (cyber review; airworthiness; approvals) versus delivery as a CDRL under DFARS.	No	No	Yes	Yes	Paper complete
	f. Software maintenance/sustainment requirements.					moved into 4biv
3	g. CDRL requirements for fundamental research programs versus CDRL needs for production/sustainment.	No	No	No	Yes	Paper complete
	i. Loss of (sustainment) support					moved into 4biv.
3. Source selection concerns.						

4	a. Data rights as an evaluation factor.	No	No	Yes	Yes	Paper complete
5	b. IP valuation versus evaluation factors and priced CLINs.	No	No	No	Yes	Paper complete
	c. Bid protest versus need to evaluate legality/business case for IP terms in proposals.					Decided to drop paper
6	d. Need for Government flexibility to use existing tools versus need for legal review of H clauses and evaluation criterion (versus 10 U.S.C. 2320; versus CICA).	No	No	No	Yes	Paper complete
4. Balancing the interests of the parties.						
	a. Funding as proxy.					
	i. Mixed funding: restore pre 2012 statutory language					Decided to drop paper
	ii. Indirect cost pools are considered privately funded					Decided to drop paper
7	iii. Treatment of IRAD versus SFRAD for IP rights determinations. 1. IRAD Risk correct for limited/restricted rights	No	No	Yes	Yes	Paper Complete
8	iv. Funding test for rights: is it the correct test or is there a less complex alternative?	No	No	No	Yes	Paper Complete
9	v. Commercial items vs noncommercial items	No	No	No	Yes	Paper Complete
b. Rights in relation to needs.						
10	i. Commercial software terms versus Government-unique requirements.	No	No	No	Yes	Paper Complete
11	ii. Authorized release and use of limited rights TD (two different points).	Yes	No	No	Yes	Paper Complete
	iii. Balance need for rights in IP versus need for competition.					Moved into 1a
12	iv. Are existing rights sufficient for depot, or is there a need for depot-specific, service specific, and program specific licenses.	No	No	No	Yes	Paper complete Includes 2b, c, d, f, and i.
5. Implementation concerns.						

13	a. Software versus technical data.	No	No	No	Yes	Paper complete. Includes 5 b, d, and i.
	b. Need to recognize differences between technical data and computer software versus need for simplified contracting.					Moved into 5a
14	c. Development versus adaptation.	Yes	No	No	Yes	Paper complete (minority position)
	d. Form, fit & function (vs. segregation/reintegration or interface) technical data; software documentation versus FFF.					Moved into 5a
15	e. OMIT versus detailed manufacturing and process data (DMPD).	No	No	No	Yes	Paper Complete
16	f. Rigid IP requirements versus need for flexible arrangements.	No	No	No	Yes	Paper Complete
17	g. Poor DID alignment with statutory/regulatory categories (FFF, OMIT, etc.).	No	No	No	Yes	Paper Complete
18	h. 10 U.S.C. 2321 protections versus complexity too high to get meaningful case law. (Link to source of funding alternatives)	No	Yes	No	Yes	Paper Complete
	i. Embedded software (the object code) versus source code (human-readable) and software design documentation (the data used to produce the object code).					Moved into 5a
19	j. Mandatory flow-down (commercial subs and suppliers).	Yes	Yes	No	Yes	Paper complete (minority position)
	k. Segregation “at the clause level”—applying non-commercial clauses to commercial TD/CS.					Decided to drop paper
	l. Right of First Refusal regarding license rights in the acquisition of spare parts					Moved into 12
6. Compliance/Administrative concerns.						
20	a. How to keep CDRL deliverable up-to-date.	No	No	No	Yes	Paper Complete

21	b. Small Business Innovation Research (SBIR) – flow down to suppliers; inability to share with primes; how evaluated.	Yes	No	No	Yes	Paper Complete
22	c. Lack of trained personnel (e.g. IP strategy; draft SNLs; DFARS 227.7103-1; IP valuation; use of CDRLs related to data)	No	No	Yes	Yes	Paper Complete
23	d. Data assertion list (7017) – burden on contractor to prepare/Government to receive versus benefit to Government; confusion over lists lead to contract delays. i. Issue: Being required to substantiate assertion within short period in proposal phase of evaluation	No	No	No	Yes	Paper complete
7. Data Acquisition concerns.						
24	a. Deferred ordering period: 6 years (rather than perpetual).	Yes	No	No	Yes	Paper Complete (minority position)
25	b. Time limits on [priced] contract options – generally 5 years, extendable to 10?	Yes	No	No	Yes	Paper Complete
	c. Deferred Ordering Part 1: data “generated or utilized” under the contract.					Moved into 7a
26	d. Deferred Ordering Part 2: all interface or major systems interface data may be ordered regardless of USG development funding.	No	No	No	Yes	Paper Complete
27	e. Failure to define and order CDRLs/reliance on deferred ordering and DAL to obtain data (Already covered, possibly repetitive).	No	No	No	Yes	Paper Complete
28	f. Deferred delivery versus escrow.	No	No	No	Yes	Paper Complete
8. Modular Open Systems Architectures (MOSA) concerns.						
29	a. GPR in MSI even if DEPE and MSI developed with mixed funding.	No	No	No	Yes	Paper Complete
30	b. GPR in interfaces developed with mixed funding.	Yes	No	No	Yes	Paper complete
	c. Open interfaces versus preference for industry standards; standards maintenance.					Decided to drop paper

9. Section 809 Panel Recommended Items					
	a. Poor alignment between 10 U.S.C. 2320 and other markings (e.g., distribution statements), clauses (DFARS 252.204-7000), and contract attachments (DIDs; DAL).				Regulatory
	b. Complexity of the IP scheme versus ability of commercial and small businesses to comply (SEC 809)				Regulatory
	c. Synchronization of sustainment policies with data rights provisions (2460 vs 2320)				Regulatory
	d. Maintaining Currency in Certifications				Regulatory
	e. Strategy and plans development: who should be engaged? Who is engaged?				Regulatory
	f. Multiple definitions of Commercial Items in Statute				Regulatory
	g. Applicability of flowing down clauses				Regulatory
	h. No definition of subcontractor and supplier				Regulatory

APPENDIX D

TENSION POINT WHITE PAPERS

1. Different Business Models in Government and Industry result in different objectives
2. Access for limited purposes (cyber review; airworthiness; approvals) versus delivery as a Contract Data Requirements List (CDRL)
3. Contract Data Requirements List (CDRL) requirements for Budget Activities 6.1 and 6.2 Research Programs versus CDRL requirements for Production/Sustainment
4. Data Rights as an Evaluation Factor
5. Intellectual Property (IP) Valuation
6. Contract Requirements in Section H Should not be treated like Standard Clauses
7. Treatment of Independent Research and Development (IR&D) versus Self-Funded Research and Development (SFR&D) for Intellectual Property (IP) rights determinations; IR&D risk correct for limited/restricted rights?
8. Is Source of Funding the Best way to Determine Rights to Technical Data?
9. Commercial vs. Noncommercial Items
10. Commercial Software License versus Government-unique Requirements
11. Authorized release and use of limited rights technical data
12. Are existing rights sufficient for maintenance and sustainment?
13. Software versus Technical Data
14. Development versus Adaptation (2 papers - a: Majority b: Minority)
15. Operation, Maintenance, Installation, and Training (OMIT) Data versus Detailed Manufacturing or Process Data (DMPD), including such data pertaining to a major system component
16. Rigid Intellectual Property (IP) requirements versus Flexible Arrangements
17. Poor Data Item Description (DID) Alignment with Statutory/regulatory Categories Form, Fit and Function (FFF) and Operation, Maintenance, Installation or Training (OMIT)
18. The Validation Process is Cumbersome and Confusing (2 papers – a: report b: line-in/line-out)
19. Mandatory flow-down (commercial subs and suppliers) (2 papers – a: Majority b: Minority)
20. How to keep CDRL deliverable up-to-date
21. Small Business Innovation Research (SBIR) (Flow-down to Suppliers; Inability to Share with Primes; Evaluation)
22. Lack of Trained Personnel
23. The Data Assertion List is a Burden on Both Contractor and the Government (Paper 23)
24. Deferred ordering period: 6 years (rather than perpetual) and Deferred Ordering Part 1: only data “generated” under the contract (2 papers – a: Majority b: Minority)
25. Time Limits on Priced Contract Options

26. Deferred Ordering Part 2: all interface or major systems interface data may be ordered regardless of U.S. Government development
27. Failure to Define and Order CDRLs (Reliance on Deferred Ordering and DAL to Obtain Data)
28. Escrow as a Form of Deferred Delivery
29. Government Purpose Rights (GPR) in Major System Interface (MSI) (Developed Exclusively at Private Expense (DEPE) or with Mixed Funding)
30. GPR in Interfaces Developed with Mixed Funding

1. Different Business Models in Government and Industry

Result in different objectives

Tension Point

Government requirements for the acquisition, long term sustainment and upgrade of weapon systems and the need for cutting edge technology, and industry's need to be appropriately rewarded for their investments create different objectives at various points in the acquisition lifecycle.

Issue

While there are many reasons for the two business models to be in conflict, this panel is charged with addressing only intellectual property (IP) issues. Over the past decade, Congress, at the behest of industry and Government, has passed a plethora of changes to the statutes that address IP. Congress created this panel in an attempt to harmonize Industry's and Government's positions regarding IP.

Discussion

The difference in business plans between Government and Industry and Government's changing needs over the acquisition lifecycle requires a change in behavior, in order to facilitate information sharing and expedite meeting of the minds at the various contract formation points in a system's lifecycle. Early in the development phase of a weapon system, the need for cutting edge technology is greater and the Government's long-term sustainment plans are not known sufficiently to determine IP needs. However, the Government should include its known needs in the solicitation provided to industry.

The lack of IP and data in later stages of weapon system acquisition/sustainment cause significant problems for the Government (e.g., inability to upgrade, replacement of parts no longer available in the market, significant price increases in the parts aftermarket, inability to compete, etc.). As the acquisition progresses from development and early fielding to sustainment, needs/business models can change. An early focus on new capability and contractor sustainment may move to competing spare parts or a desire to move work to a Government depot. By providing long-term sustainment information, industry has an opportunity to respond to the Government's needs, invest accordingly and potentially offer licenses and data that meet those needs.

While the Panel's focus is on 10 U.S.C. 2320 and 2321, there were extensive discussions regarding other statutes that address the requirements for competition, Government depot requirements, fair and reasonable pricing, and meeting Warfighter requirements. It is not the Panel's intent to recommend changes to other statutes, but the Panel understands, from a Government perspective, that developing a strategy for IP for a weapon system entails consideration of multiple statutes surrounding a variety of topics that include competition, depot maintenance, "green," Small Business Innovation Research (SBIR) and small business. The Panel met with the Section 809 Panel and suggested several areas that the 809 Panel might review. They included the varying definitions of "commercial item" and "maintenance" in statute; flow-down of contract terms; recurring training needs; the need for better guidance on long-term sustainment plans and strategies; and Government depot requirements for hardware and software.

Industry Panel members maintain that if the Department of Defense (DoD) wants to "encourage industry investment in new technologies, products, and processes relevant to DoD requirements" and have "access to industry innovations developed for commercial use," then the DoD must be willing to accept the same IP rights accorded to commercial buyers or be willing to pay the "value" industry gives up by providing additional IP rights. This potentially presents a dilemma to the Government. First, it would require including additional funds for IP rights. Second, it might require the DoD to rethink its long term sustainment strategies. Third, it may eliminate the ability to bring work into depots and fourth, it may drive noncompetitive procurements to a later stage in the weapons system life cycle.

The criteria and scope of government purpose rights (GPR) also create issues with business models. GPR attaches (mixed funding rule) with any level of Government funding. In addition, industry views the scope of GPR to be quite broad covering all government agencies, government contractors and any government purpose, and is indistinguishable from unlimited rights for defense specific technologies. The prospect of GPR may deter industry from making investment in new products or processes, and the potential for GPR may deter non-traditional defense contractors from offering non-developmental items that require modifications at government expense.

In addition, the default sunset of GPR to unlimited rights in five years is an issue for industry since many products may well have IP investment recoupment periods that extend well beyond five years.

The Panel had extensive discussions on IP valuation models. It is clear there are as many ways to value IP as there are companies in industry. The common thread, though, in all the discussions was industry does, in fact, make conscious decisions to invest in new products, technologies, or processes that include determining a "value" or return on investment. The Panel

recognized that IP valuation is not taught in any of the DoD acquisition courses required for certification in any of the Defense Acquisition Workforce Improvement Act competencies. Further, due to the many various ways IP may be valued by industry, the Government's practice of asking for a price for IP in solicitations has the potential to "skew" total evaluated price. The Panel was presented one Government solicitation where, rather than asking for a price for IP, the Government determined the long term difference in sustainment cost based on whether or not certain IP rights were provided and used that figure to determine total evaluated price. (See Tension Paper 3a.)

The Panel was provided examples where the DoD, in competitive acquisitions, requested unlimited rights or GPR at all levels of the supply chain regardless of funding or asked firms to give up their SBIR data rights. The Panel believes the problem here is lack of training and lack of understanding the basic tenets of DoD's IP policies. (See Tension Paper 6c.)

The Panel discussed Specifically Negotiated License Rights (SNLR) many times. It is the Panel's opinion that the Government, as a rule, believes SNLR is viewed as an exception. The truth, however, is the Government is encouraged to use SNLR when it makes sense in any given acquisition. It is industry's opinion that many IP issues could be solved if industry better understood the Government's long-term sustainment needs and if they were asked to offer SNLR to meet those long-term needs.

The Panel believes the Government must seek to identify its long-term requirements and articulate them in the Request for Proposal, to the degree possible. This includes technology insertion, upgrade, spare parts procurement, depot maintenance objectives, obsolescence, and system sustainment. To do this there must be a requirement to articulate these needs in planning documentation. The Panel could not identify in any DoD directive the requirement to address these long-term requirements.

Lastly, in addition to the Government's need to address long-term sustainment in acquisition, upgrade, and sustainment plans, the Panel received information that indicates a need to balance data deliverables from the front-end to the back-end of a program's life cycle: greater data demands at the outset of the acquisition of a platform can reduce competition during the acquisition phase and the failure to obtain sufficient data at the acquisition phase can reduce competition during the upgrade and sustainment phases.¹

¹ At least one pre-award protest was sustained based on the impact of requiring rights in technical data which reduced competition (American Safety Council, Inc. v United States, 122 Fed.Cl. 426 (Fed Cl. July 24, 2015), and there are news articles which indicated competition was reduced based on requirements in solicitations (Tom Osborne, Intellectual Property Concerns Swayed EADS JMR Pullout, Aviation Week (Jun 24, 2013); Jon Harper, Acquisition Process Undermining Silicon Valley Outreach Efforts, pp. 23-25, National Defense (June 2016)

Recommendation

The panel recommends no statutory changes to U.S.C 2320 or 2321.

We recommend the following changes to the Defense Federal Acquisition Regulation Supplement or relevant Department regulations:

- 1) Include in the solicitation the Government's known long-term requirements (e.g., technology insertion, upgrade, spare parts procurement, depot maintenance objectives, obsolescence, and system sustainment). Ask offerors to provide licenses, data deliverables and/or design alternatives that meet the Government's expressed objectives.
- 2) The Government should prioritize its objectives, share the priorities with industry (e.g., technology insertion/upgrade, spare parts procurement, depot maintenance, obsolescence and system sustainment) and address each separately to improve the Government's ability to meet its objectives.
- 3) When mixed funding exists in a product development, the Government should consider either extending the period for GPR or negotiate a SNLR that more appropriately recognizes the parties' relative contributions.
- 4) When the Government seeks additional deliverables or rights beyond the standard or default licenses, to include SBIR data rights, then the Government should negotiate a fair and reasonable price for those deliverables or IP rights it obtains based on best practices, standards, or norms.
- 5) Include guidance to align the acquisition, upgrade and sustainment plans to ensure the data delivery and licensing requirements consider potential impact on competition caused by broad data delivery and licensing requirements. The guidance may consider an industry best practice in which the program discusses the IP needs with the potential suppliers, in advance of the initial acquisition, to determine which IP approaches are most likely to maximize competition, capability to upgrade and sustainability for each major system and component over the lifecycle of the product while also meeting the program's identified needs for technical data and computer software delivery and rights, and program cost.

2. Access for limited purposes (cyber review; airworthiness; approvals) versus delivery as a Contract Data Requirements List (CDRL)

Tension Point

While DFARS part 227 provides guidance on the acquisition of formal CDRL deliverables, it does not provide instructions on the use of contractor data where a formal CDRL is not appropriate or possible.

Issue

The Panel noted that certain data received by the Government is not needed for long-term sustainment or upgrades. In these cases, industry has objected to a formal CDRL delivery with markings compliant with DFARS 252.227-7013 or 7014. The Government has other needs for review of contractor data, including review of draft CDRLs or draft IPT documents; airworthiness data to validate the safety of an aircraft; review of supplier data by Defense Contract Management Agency (DCMA) or Defense Contract Audit Agency (DCAA) to validate contractor contractual compliance; contractor data used in a commercial item determination review process; IRAD technical interchanges under DFARS 231.205-18(C)(iii)(c)(4)¹; and cyber investigations under DFARS 252.204-7012. There is also a lack of instruction on how the Government is able to receive such data (except in the case of proposals which have established marking and protection systems such as those in Federal Acquisition Regulation (FAR) 15.609 or FAR 52.215-1). The lack of guidance can lead to unnecessary confusion over the proper marking of such data, and lead to delays in program execution.

There have also been discussions on the Government's avoidance of non-disclosure agreements, which are customary industry mechanisms to allow limited review of data for a specific purpose. While the Government typically cites the Trade Secrets Act, 18 U.S.C. 1905 as effectively providing a non-disclosure agreement, industry notes this statute does not provide a private civil cause of action against the Government. While it is arguable there are other causes of action, to attract non-traditional contractors who are used to working and negotiating non-disclosure agreements, industry believes that DFARS should provide instruction to the contracting officer on the use of such agreements to facilitate this exchange.

The Panel received information from commercial industry which has used other access mechanisms to comply with validation requirements. For instance, where cybersecurity reviews are needed, trusted third parties such as FedRamp could be used to validate for the customer that the software meets their requirement (and provide the results to the customer) without providing

¹ This requirement has been suspended due to Class Deviation 2017-O0010 as of September 14, 2017

the customer access to the software source code. Where a third party is not available, the Department could create a process where contractors hand carry computers or discs to specific Department labs or agencies for analysis, and the contractor would maintain visual control over the data/software while the Department performs tests, scans source code, and the like. Where validating airworthiness or performing frozen planning, the Government could do what is similarly done in commercial aviation in which Federal Aviation Administration officials are given access to contractor facilities to review sensitive original equipment manufacturer data without being provided copies.

Lastly, the Panel discussed the use of subscription agreements for access to data, such as software as a service. The current DFARS data rights clauses do not apply to such agreements since, in these cases, the technical data or computer software is not delivered to the Government. Such agreements tend to allow the end user to use information in a particular data set or software over a network for defined purposes. The DFARS should provide guidance on these subscription agreements.

Recommendation

The Panel recommends no change to 10 U.S.C. 2320 or 10 U.S.C. 2321 to address this issue.

The Panel recommends the Department propose regulatory language which would allow the Government to appoint a contracting officer or other personnel to sign a non-disclosure agreement or obligation, and delineate the conditions under which they can be signed.

The Panel recommends the following changes to the DFARS relative to bailment or access:

DFARS 227.7103-1, Policy.

(a) DoD policy is to acquire only the technical data, and the rights in that data, necessary to satisfy agency needs.

(b) Solicitations and contracts shall—

(1) Specify the technical data to be delivered under a contract and delivery schedules for the data; or where delivery is not required, the types of contractor data access or software subscription agreements which the contractor could propose to meet the Government's needs;

DFARS 227.7103-2, Acquisition of technical data.

(b)(1) Data managers or other requirements personnel are responsible for identifying the Government's lifecycle minimum needs for technical data, including whether the technical data must be delivered or only accessed for limited purposes. Data needs must be established giving consideration to the contractor's economic interests in data pertaining to items, components, or processes that have been developed at private expense; the Government's costs to acquire, maintain, store, retrieve, and protect the data; reprocurement needs; repair, maintenance and overhaul philosophies; technical insertion, modernization and upgrade; spare and repair part considerations; and whether procurement of the items, components, or processes can be accomplished on a form, fit, or function basis. When it is anticipated that the Government will obtain unlimited or government purpose rights in technical data that will be required for competitive spare or repair parts procurements, such data should be identified as deliverable data items. Reprocurement needs may not be a sufficient reason to acquire detailed manufacturing or process data when items or components can be acquired using performance specifications, form, fit and function data, or when there are a sufficient number of alternate sources which can reasonably be expected to provide such items on a performance specification or form, fit, or function basis. When the data needs are limited to review or audit purposes (including by DCAA or DCMA), the requirements personnel should consider use of data access, bailments or subscription agreements.

(c) Contracting officers are responsible for ensuring that, wherever practicable, solicitations and contracts—

(6) Identify the type and quantity of the technical data where limited access is required instead of delivery, who would have such access, and for what purpose. To the maximum extent possible, limited access is required, the Government should use contractor data access or software subscription agreements which meet the Government's needs under the contract. Limited access shall be presumed where the Government use is limited to validation of contractor contractual compliance; contractor data used in a commercial item determination review process; and IRAD technical interchanges under DFARS 231.205-18(C)(iii)(c)(4)

Like changes should be made to DFARS 227.7203.

Exclude cyber investigations under DFARS 204.73 from the scope of DFARS 227.71 and 227.72.

The Panel also recommends that the Department consider delegating to the Military Departments and Defense Agencies the authority to create access agreements or clauses which allow for delivery of data with less than Limited or Restricted Rights at specific Department of Defense component locations for specific purposes, such as airworthiness determinations for use where

delivery is necessary. Such specific purpose access agreements or clauses should be structured to have—

- their own marking requirements to distinguish the data provided for the specific purpose from data delivered under normal DFARS licenses (such as for bids and proposals in FAR 15.609 or FAR 52.215-1), and consider whether marking of physical containers instead of the data itself should be an option where there is a need for expediency; and
- ensure that they apply only to the set of documents provided under the specific purpose, and do not change either parties' license rights in deliveries made or to be made outside of the specific delivery.

3. Contract Data Requirements List (CDRL) requirements for Budget Activities 6.1 and 6.2 Research Programs versus CDRL requirements for Production/Sustainment

Tension Point

Standard Defense Federal Acquisition Regulation Supplement (DFARS) data rights and CDRLs are inappropriate for intellectual property for research contracts.

Issue

The Panel received some comments on whether the same data rights clauses used for production and sustainment are appropriate for Budget Activities 1 and 2 (Basic and Applied Research) research and development. Specifically, the current DFARS clauses for rights to technical data and computer software have major parts that are inapplicable for situations where the developed parts or code would never be directly put into production, competed or maintained. In these contracts, the results are interim and final reports demonstrating whether the research is promising.

Further, research institutions, small companies, and non-profits that should be approached to perform research work for the Government do not have staff members sophisticated in DFARS policies and procedures, leading to potential compliance problems.

The Panel received testimony that Department of Defense (DoD) research entities using Other Transaction authority were able to use simplified data rights clauses which research institutions largely accepted. The guidance in the DoD Grant and Agreement Regulations also provides guidance on minimal data rights requirements in a research contract.

Government members did note that the Government needs to at least document development of technology under these research agreements where the technology is being reused in production contracts. Therefore, to the extent that a large technical data package is ordered, it is used for archival purposes as opposed to downstream maintenance of any items or software developed under a research contract. In this sense, the need for a technical data package is more consistent with the patent rights reporting requirements of subject inventions under Federal Acquisition Regulation (FAR) 52.227-11 or DFARS 252.227-7038 since both reporting requirements document government involvement in development of technology.

Recommendation

The Panel does not recommend any statutory changes to 10 U.S.C. 2320 or 2321.

The Panel does recommend the DoD consider a streamlined data rights clause to simplify the requirements, consistent with the minimum requirements included in Other Transactions and the guidance in the DoD Grant and Agreement Regulations. The DoD should ensure such clauses include the ability to agree to specifically negotiated licenses to tailor the clauses when used in research contracts to attract the most research institutions to compete for research contracts. Where used, such clauses should be used instead of DFARS 252.227-7013, 252.227-7014, or 252.227-7015 such that a single clause governs data rights for the research contract.

The Panel further recommends that the DoD Grant and Agreement Regulations, DoD 5010.12-M, and associated Data Item Descriptions be changed to ensure research data requirements include a mechanism for archiving technology development for the Budget Activities of Basic and Applied Research (6.1 and 6.2), including listing of technologies developed at the lowest practicable and segregable level. The Panel suggests that such requirements could be accomplished while simultaneously forcing compliance with FAR 52.227-11 and DFARS 252.227-7038 if the requirements incorporated the subject invention reporting requirements into the formal CDRLs to help document technology concepts developed with Government funding, such that a contractor who submits an interim or final research report is also complying with the patent reporting requirements in FAR 52.227-11 and DFARS 252.227-7038.

4. Data Rights as an Evaluation Factor

Tension Point

Source selections in the past often failed to include an evaluation factor for technical data or computer software (collectively, “data”), and the associated license rights (a.k.a. “data rights”), so the value of intellectual property in an innovative proposal was overlooked or not used to discriminate among proposals. A recent trend in source selections is to include provisions seeking a certain level of data rights, e.g., Government Purpose Rights (GPR), for all deliverable data, with no ability for industry to trade off the sought-after level of data rights for another benefit to the Government, such as reduced cost of a commercial product or increased innovation in the proposed solution. Industry perceives this trend as an arbitrary use of competitive pressures to obtain unnecessarily broad licensing terms, which discourages industry investment and may be contrary to 10 U.S.C. 2320(a)(2)(H) or 15 U.S.C. 638(j)(2).

Discussion

It is an inherently governmental function for the Government to determine its requirements and to select the evaluation factors that it will employ during a source selection in order to reach the “best value” determination while ensuring such evaluation factors drive multiple offers in satisfaction of competition requirements. This concept has been confirmed repeatedly by the General Accountability Office in its bid protests decisions. To carry out their missions and to meet certain statutory requirements (e.g., Competition in Contracting Act), Government agencies require access to certain data either from an original equipment manufacturer (OEM) contractor or subcontractor, or generated from Government sources. Government agencies are required by statute to always evaluate price or cost during a source selection. Since two thirds of the price/cost of an item typically occurs in the sustainment phase of the acquisition, Government agencies need to identify the necessary data and intellectual property licenses in the necessary data during a source selection, and should be accounting for such intellectual property to accurately assess the total lifecycle cost/price of the item from each bidder in the competition.

The Department of Defense (DoD) must respect the cutting-edge technology of innovative companies, particularly where the technology was developed with private investment. When a private company is not willing to share proprietary details regarding its technology with the DoD at any price, the DoD may seek a different technical solution – one that enables organic or competitively-awarded life-cycle sustainment and modernization of the item.

The Panel discussed that the Government cannot require potential contractors to relinquish to the Government, as a condition of contract award, data rights greater than those authorized by 10 U.S.C. 2320 or 15 U.S.C. 638(j)(2). Under these provisions, DoD cannot include a proposal or

bid requirement that the winning contractor must grant the Government a broad license, such as GPR, when the statutory regimes would allow the contractor to assert a more restrictive license, such as Limited Rights, Small Business Innovation Research (SBIR) data rights, or commercial license rights. The Panel reviewed the history of 10 U.S.C. 2320, which was enacted, in part, to protect industry from certain DoD practices which industry believed discouraged industry investment incentives and competition. Industry members also noted to the Panel that even expressing a preference for specific Defense Federal Acquisition Regulation Supplement (DFARS)-defined license rights may chill competition. The industry Panel members support an expansive interpretation of the concepts included in 10 U.S.C. 2320(a)(2)(H) or 15 U.S.C. 638(j)(2), which they perceive as encouraging competition and private investment.

The Panel also discussed DoD's needs to find a way to evaluate the data licenses each offeror proposes for a contract, and notes that 10 U.S.C. 2305 discusses the use of evaluation of data licenses in specific situations. The Government Panel members believe, the correct balance is to allow evaluation of each offeror's data deliverables and associated licenses during source selection, which may provide a better value for the Government and, since the offerors are voluntarily proposing the data licenses, the Government is not forcing a particular offeror to give up any license rights in violation of 10 U.S.C. 2320(a)(2)(H) or 15 U.S.C. 638(j)(2).

Industry has previously proposed that the DoD be prohibited from evaluating a contractor's proposal based on the contractor's willingness to relinquish greater rights than the Government is entitled to require under the law. This proposal was born of practices which industry believes effectively devalued intellectual property to the extent that it deters private investment in military technologies, and also increased bid and proposal prices with little benefit.

The Panel noted that past source selections often failed to include an evaluation factor for data deliverables, and associated data rights, so the value of intellectual property in an innovative industry proposal may be overlooked or not used to discriminate among proposals. In other source selections, the *quantity*, instead of the *quality*, of data deliverables and data rights was evaluated, which may result in 1) a more expensive solution in terms of total life cycle costs, and 2) a less innovative solution being offered and selected instead of more innovative, commercial or proprietary, solutions that deliver less data and data rights but provide substantially greater cost savings over the acquisition life cycle.

The Panel also discussed one recently used model where the evaluation factor assigned a monetary value that reduced the total evaluated price of offers that provided at least GPR for a set of listed components. Under this model, offerors received a benefit for ensuring the Government received license rights to allow the data to be used for competitive life-cycle support, and the offeror was effectively given a competitive benefit if it offered the sought-after license right. The Panel noted that such an example has potential downsides since lower-tier

suppliers (especially those providing commercial or entirely privately developed technologies) are unlikely to agree to such terms even if the prime offeror is willing; if there are lower-tier supplier exceptions, the evaluation scheme provides greater rights from vertically integrated companies who use fewer suppliers which is not considered in the evaluation factor; and the evaluation factors need to account for the actual value received as compared to the default rights. The model highlights the issues which need to be balanced to ensure best value for the Government and fairness to the offerors.

The Panel further noted that the DoD has failed to provide uniform source selection procedures for the evaluation of data deliverables and data rights, preferring instead to leave this decision with program personnel who can tailor requirements to the needs of individual programs. The Panel is also concerned that there is a lack of DoD-level or agency-level oversight of these individually tailored source selections. The Panel believes that DoD source selections should consistently communicate the Government's acquisition and sustainment requirements in clear, meaningful ways to encourage Industry to propose the best possible array of noncommercial and commercial solutions (including intellectual property). In turn, this allows the Government to make meaningful distinctions amongst those disparate proposals, and ensure that the award represents the best value to the Warfighter and the Nation. DoD has also not evaluated the increased bid and proposal costs associated with complex evaluation factors, and has not provided guidance on intellectual property valuation techniques which allow the evaluation factors to bear a meaningful relationship to the market value of the data licenses to prevent over or under payment for such licenses. The DoD has also not provided guidance on when such evaluation factors might not be appropriate, such as where source selection is by other than best value involving trade-offs (e.g., intellectual property may be harder to evaluate or discriminate meaningfully when using lowest price technically acceptable procedures). Also, there is no guidance on allowing offerors to submit counter proposals which may result in improved technical data packages with license rights tailored to the Government's actual needs, as opposed to using Government Purpose Rights as the only possible choice.

The DoD should not adopt a "one size fits all" approach to intellectual property evaluation in source selections. Clear criteria to meaningfully discriminate between offers using data licenses as an evaluation factor should be provided to offerors, such as reduced cost and schedule of development from commercially available items, or reduced sustainment costs when the Government receives sufficient data deliverables and data rights for organic sustainment, the intellectual property valuation techniques used by the Government, and the analysis of the effect on cost/price due to the effects on competition caused by increased license requirement. Source selections should be carefully structured to avoid "paying more than once for" the value of intellectual property and should be structured in a way that does not devalue industry's ability to provide innovative solutions.

The Panel believes industry feedback should be actively encouraged on evaluation factors and the Government should incorporate the feedback to ensure the factors represent the best value to DoD for a given solicitation as informed by the Intellectual Property Strategy adopted by the program under DoD Instruction 5000.02. The offerors should provide a detailed discussion of their intellectual property valuation techniques and assumptions and should also be made aware of any formulas used by the Government in calculating the evaluation factors which often reveal subtle preferences offerors need to be aware of to meet the Department's needs. Industry's view is the lack of pre-award protest is not indicative of the appropriateness or effectiveness of the evaluation factors. Post award, Government debriefings should provide offerors the key aspects of how their offer was evaluated under the evaluation factor using the same formulas and assumptions used for all proposals in order to have meaningful feedback.

Recommendation

The Panel recommends no change to 10 U.S.C. 2320 or 10 U.S.C. 2321 to address this issue.

The Panel recommends a new section in the Fiscal Year 2020 (FY20) National Defense Authorization Act (NDAA), section 8xx regarding a pilot program for intellectual property evaluation in acquisition planning and source selection regarding certain Major Defense Acquisition Programs, as follows:

FY20 NDAA, section 8xx PILOT PROGRAM ON INTELLECTUAL PROPERTY EVALUATION FOR MAJOR DEFENSE ACQUISITION PROGRAMS

(a) PILOT PROGRAM.—Not later than 180 days after the date of enactment of this act, the Secretary of Defense and the Secretaries of the military departments may jointly carry out a pilot program to assess mechanisms to evaluate intellectual property (e.g., technical data deliverables and associated license rights), including commercially available intellectual property valuation analysis and techniques, in the major defense acquisition programs for which they are the milestone decision authority to better understand the benefits associated with these techniques on—

- (1) The development of cost-effective intellectual property strategies, and
- (2) Assessment and management of the value and costs of intellectual property during acquisition and sustainment activities (including source selection evaluation factors) throughout the acquisition lifecycle for any major defense acquisition program selected by the Secretary concerned.

(b) ACTIVITIES.—Activities under the pilot program may include the following—

- (1) Establishing a team of Department of Defense and private sector subject matter experts to identify, to the maximum extent practicable at each milestone for the selected major

defense acquisition programs, intellectual property evaluation techniques to obtain quantitative and qualitative analysis related to the value of intellectual property during the procurement, production & deployment, and operations & support phases of the acquisition of the systems under the program.

(2) Assessment of commercial valuation techniques for intellectual property for use by the Department of Defense.

(3) Assessment of feasibility of agency-level oversight to standardize intellectual property evaluation practices and procedures.

(4) Assessment of contracting mechanisms to speed delivery of intellectual property to the Armed Forces or reduce sustainment costs.

(5) Assessment of agency acquisition planning to ensure procurement of intellectual property deliverables and intellectual property rights necessary for Government-planned sustainment activities.

(6) Engagement with the commercial industry to—

(A) Support the development of strategies and program requirements to aid in acquisition and transition planning for intellectual property;

(B) Support the development and improvement of intellectual property strategies as part of life-cycle sustainment plans; and

(C) Propose and implement alternative and innovative methods of intellectual property valuation, prioritization, and evaluation techniques for intellectual property.

(7) Recommend to the cognizant program manager for a major defense acquisition program such evaluation techniques and contracting mechanisms for implementation into the acquisition and sustainment activities of that major defense acquisition program.

(c) ACQUISITION OF COMMERCIAL, SMALL BUSINESS INNOVATION RESEARCH-DEVELOPED, AND NONDEVELOPMENTAL ITEMS, PRODUCTS, OR SERVICES.—The pilot program shall provide criteria to ensure the evaluation of Small Business Innovation Research (SBIR)-developed products, commercial items, and nondevelopmental items are appropriately considered against items to be specifically developed for the major defense acquisition program and the benefits of reduced risk regarding cost, schedule and performance of commercial, SBIR-developed, and nondevelopmental items, products, or services are appropriately valued.

(d) ASSESSMENT.—Not later than one year after the commencement of the pilot program, and annually thereafter through 2023, the Secretaries concerned shall provide on July 1st of that year through the Secretary of Defense to the congressional defense committees a joint report on the pilot program required under paragraph (a) of this section. The report shall, at a minimum, include,—

(1) A description of the major defense acquisition programs selected by the Secretary concerned;

- (2) A description of the specific activities in paragraph (b) that were performed under each program;
- (3) An assessment of the effectiveness of the activities;
- (4) An assessment of improvements to acquisition or sustainment activities related to the pilot program; and
- (5) An assessment of cost-savings from the activities related to the pilot program, including any improvement to mission-success during the operations & support phase of the program.

(e) AVAILABILITY OF FUNDS.—The Secretary of Defense and the Secretaries of each of the Military Departments are authorized to expend funds to carry out the pilot program in paragraph (a) from funds authorized and appropriated to the Department of Defense for fiscal years 2018 through 2025.

(f) SUNSET.—The authority to carry out the pilot program under this section shall expire on September 30, 2025.

The Panel recommends the Department draft regulations to be implemented when using intellectual property as an evaluation factor which reflect a common set of principles and procedures for competitive source selections. Such principles should include:

- Avoiding use in source selections when there is limited ability to meaningfully discriminate between varying intellectual property proposals (e.g., intellectual property may be harder to evaluate or discriminate meaningfully when using lowest priced technically acceptable procedures).
- Transparency to all offerors as to the evaluation factors and the calculation of the data rights license value affecting the evaluation factors based on identified valuation techniques.
- Ensuring such evaluation factors do not unnecessarily limit commercial and non-commercial competition, and are in compliance with the spirit of 10 U.S.C. 2320(a)(2)(H), 15 U.S.C. 638(j)(2), and 10 U.S.C. 2305.
- Ensuring the evaluation factors allow for multiple license rights offerings to meet specified Government objectives for the use of such data, including requirements for Modular Open Systems Approaches, interfaces, and long term sustainment and upgrade needs at specific locations and agencies.
- Ensuring such evaluation factors account for commercial items, SBIR products, and supply chain issues in requiring specific license rights.
- Ensuring such evaluation factors shall consider only license rights the DoD actually needs to perform its mission, to ensure return on its technology development investments, and to account for the Government's existing licenses to prevent effectively paying twice for the same intellectual property.

- Ensuring the valuation of rights when used in an evaluation factor shall be assessed in accordance with best practices and consensus based standards and norms, by DoD personnel who have received extra training in valuation techniques or are experts in the field of intellectual property valuation.

The Panel recommends such factors be incorporated into the DFARS, and the DoD establish a panel of intellectual property valuation and financial analysis experts within DoD to determine (or to vet methodologies used to determine) relative values of sustainment solutions and intellectual property rights over a product's life cycle to aid in evaluating such factors.

The Panel recommends DFARS part 212 and DFARS 215.506, respectively, include a new section on debriefings for evaluation factors which evaluate data rights licenses. The new section needs to ensure offerors are given full access to proposal neutral facts used by the Government and applied to all the offers for the same evaluation factor, including any formulas and valuation assumptions used by the Government in such evaluations.

The Panel recommends an update to the guidance in Defense Acquisition Guidebook at <https://dag.dau.mil/> and Department of Defense Source Selection Procedures to recognize and reinforce the necessity to use, when appropriate, intellectual property, as an evaluation factor. Mandate that DoD component (e.g., Defense Advanced Research Projects Agency, Army, Navy, Air Force) guidance on source selection be updated accordingly. The Panel recommends that the Department obtain, post award from offerors, information on the amount of time and effort required to comply with proposal evaluation factors based on intellectual property, and update this guidance to minimize the impact.

5. Intellectual Property (IP) Valuation

Tension Point

DoD requires sufficient rights to technical data to upgrade and sustain its systems and to compete future acquisitions. There is no current agreement on how to value IP and thus determine a fair and reasonable price. This creates problems in both competitive and non-competitive situations.

Discussion

Many articles and books have been written on the most appropriate methodologies for valuing IP across a wide diversity of circumstances and fact patterns. There are many experts in the field of IP valuation, employed by a wide variety of boutique specialty firms, international financial consulting and accounting firms, and government agencies. As a result of regulation developed by the Federal Trade Commission, the Securities and Exchange Commission, the International Trade Commission, the Internal Revenue Service, and case law developed by the courts, and innovations developed by IP valuation experts inside and outside academia, there is a remarkable body of best practices available to students and practitioners.

Two organizations have developed and are developing standards in the field of IP valuation. The first is an already existing standard on the valuation of trademarks and brands that was developed by the International Organization for Standardization (ISO) entitled, “ISO 10688: Brand Valuation—Requirements for Monetary Brand Valuation.” The second is a standard being developed by LES Standards, a voluntary consensus standards body, which is part of the non-profit, professional association called the Licensing Executives Society USA and Canada, or LES. LES Standards has been accredited by the American National Standards Institute (ANSI), the unique body in the US that accredits voluntary consensus standards developers. ANSI has accredited over 250 such organizations, such as IEEE, ASTM, SAE, and the AMA. LES Standards is developing an IP valuation standard that should undergo broad review and comment toward the end of 2018 and that is projected to be issued as an ANSI standard in 2019.

An issue for DoD and its industrial partners is that in many cases, neither DoD program offices nor their potential industrial partners, are aware of best practices in the field of IP valuation and are not aware that a standard is being developed that attempts to capture those best practices in a singular document.

In the competitive phase, DoD has the most leverage to obtain the IP rights it is interested in at a fair and reasonable price. Since DoD has difficulty articulating, prior to development, its long term sustainment strategy, it frequently requests broad rights such as government purpose

rights or unlimited rights. Granting DoD rights either in commercial technology or technology otherwise developed exclusively at private expense can destroy the value of that IP. Paper 4 addresses IP as an evaluation factor in competitions.

Once a contract is awarded issues also arise when contractors identify new data assertions during program performance, such as when new information is introduced, or, when DoD changes its technical requirements or sustainment strategy.

The Panel believes in both the competitive and non-competitive situations solutions likely exist that will meet DoD's requirements, will not deter commercial firms from participating in the market place and will provide a fair and reasonable return to industry on its IP investment.

Paper 16 recommends greater use of specially negotiated license rights and the potential for additional IP license templates to be provided to the acquisition community. Potential examples are 1) breaking the IP strategy into five elements: upgrade, spare parts, Government only depot maintenance, depot maintenance with third party contractor support, and third party commercial support; 2) defining for each element the Government's requirement; 3) the use of escrow accounts (paper 14), 4) limiting GPR like licenses to just the specific program or to the specific Service of DoD and 5) use a company's existing commercial license as the base and make the minimal changes necessary to meet DoD requirements. Approaches such as these would meet DoD's requirements, limit the availability of industry's IP to third parties, and leave intact much of the value of industry's IP and thus reduce the amount DoD would pay to get the necessary rights.

Whether or not DoD seeks to use SNLR as suggested above, when either industry identifies new data assertions after contract award or when DoD changes its requirement or sustainment needs, the parties have struggled to determine a fair and reasonable price for the IP. The Panel believes training needs to be developed for the acquisition community that addresses how industry values IP and determines a reasonable return for its investment.

Contracting officers are tasked to develop solutions and prices that are fair to both parties. To do so, they must understand how commercial firms value their IP. Today, if the contracting officer and a company cannot reach agreement, the contracting officer can issue a final determination. The company can file suit in the Federal Court of Contract Appeals to have the determination adjudicated. To avoid such an action, the Panel believes contracting officers should be directed to consider commercial guidelines and standards that are widely accepted to find solutions that work for both parties.

Because of DoD's unique mission, it often has legitimate needs for IP rights that are beyond those provided commercially. Potential solutions might be to limit the rights sought to the particular program or to limit the rights to particular uses or for limited periods of time on that program. This would limit the value of rights destroyed for the commercial firm to that program alone, and it might be sufficient to limit the price that DoD would pay (and that the industry partner would expect) for those rights to the bare minimum. Doing so would provide DoD's

industrial partners with adequate compensation for granting such rights, without breaking the bank. Such partners, having been fairly compensated, would then have no reason to avoid DoD in the future, but would rather seek to serve DoD, since they would have the expectation of fair compensation in the future for the commercially unusual rights DoD needs.

Recommendation

The Panel recommends no changes to 10 U.S.C. 2320 or 10 U.S.C. 2321 to address this issue.

The Panel does recommend the following changes be made:

1. Develop a DAU course on IP valuation that covers best practices and available standards.
2. Consider the value of DoD's IP needs in Government estimates.
3. Require contracting officers to consider commercial IP valuation practices and standards when determining a fair and reasonable price for the requested IP.
4. Include IP as a topic in industry day presentations when appropriate.
5. Require industry to provide the basis for their requested IP valuation that is consistent with best practices, norms, and standards in the field of IP valuation.
6. DoD should provide comment to LES when they publish their standard for approval.

6. Contract Requirements in Section H Should not be treated like Standard Clauses

Tension Point

The Government may, at times, include special requirements in its solicitations to address its needs regarding technical data, computer software, and/or licensing arrangements, which industry is concerned may be an unauthorized deviation.

Issue

The Government has the right to include special contract requirements (SCRs)¹ in Section H of its solicitations and contracts. However, industry believes some of these SCRs are inconsistent with the DFARS or resemble “local clauses” that should be subject to rulemaking. The Government and industry do not always agree on when an SCR warrants such treatment.

Discussion

Some SCRs for technical data and computer software have been used in multiple contracts in similar format or with some alteration. Although the Government has the right to include SCRs in its solicitations, there are times that such requirements may rise to the level of a “local clause” that also requires clearance through the rulemaking process.

The Panel received comments from industry related to the use of SCRs, which can be summarized as the following:

- Agencies have been issuing SCRs in essentially the same form, which effectively creates a new standard clause without undergoing the administrative process of notice and comment normally afforded to standard clauses. Even where the SCR have existing authority, they are not subject to the public rule making process and may reduce competition, have unintended consequences, and may increase the burden for compliance under the Paperwork Reduction Act.
- SCRs sometimes conflict with DFARS clauses or regulations, such as requiring enhanced data assertion lists which include requirements beyond DFARS 252.227-7017, requiring contractors to give up rights in computer programs deemed “OMIT”, adding specific requirements for commercial software licenses contrary to DFARS 227.7202, not accounting for SBIR data rights, or providing for automatic ordering off of a Data Accession List instead of using the process contractually required under DFARS 252.227-7027. In these cases, industry comments indicate these are “deviations” as

¹ These contractual terms can sometimes be included in the Statement of Work

defined in FAR 1.401, for which Defense Procurement and Acquisition Policy (DPAP) approval is required per DFARS 201.402.

Industry and Government do not always agree on when the rule-making process is required. Clearly, when a requirement is inconsistent with the FAR or DFARS, either a deviation under FAR 1.401 or rulemaking is required. In other cases, the requirements provide procedural information related to the handling of issues in source selection or contract administration. Such requirements aim to alleviate confusion and to reduce administrative issues for a particular acquisition and do not require rulemaking.

Regarding data rights, SCRs are often used as a mechanism to implement SNLRs. The Panel has also discussed at length that it may well make sense to create additional IP license templates. Industry has experienced with the Services and Agencies creation of additional IP licenses or clauses, unique from DFARS Part 252.227 clauses that are used as a template for multiple procurements. It appears that these licenses or clauses have not gone through public rulemaking (see FAR 1.301, DFARS 2.301) to become an official, approved, repetitive use clause, assuming that is necessary. That is, the Government members are not convinced that use of these templates requires the public rulemaking process.

The Panel does not want to discourage the use of template as a negotiation starting point for SNLRs or place unnecessary hurdles to meeting the special requirements of a particular acquisition. The Panel does believe, however, a better description of when a special requirement rises to the level of a “local clause” that requires rulemaking would be beneficial to clarify this hazy area of the public procurement process. As such, the Panel makes the following recommendations:

Recommendation:

The Panel does not recommend any changes to 10 U.S.C. 2320 or 2321.

The Panel recommends the implementing regulation for the Cadre of Experts created by 10 USC 2322 be tasked to:

- a. Clarify when a special requirement for technical data and computer software may warrant clearance through the rulemaking process and recommend to DPAP any suggested updates to the DFARS for making this requirement clearer.
- b. Develop negotiable templates for SNLRs within the authority of DFARS 252.227-7013 and 252.227-7014 (including specifically negotiated license rights authorized by DFARS) that do not require rulemaking. In developing these templates, the Cadre should:
 1. Review existing and in use Service and Agency unique requirements or provisions and develop, as appropriate, additional licenses for consideration by the acquisition workforce, consistent with the Cadre’s mandate “to ensure a consistent, strategic, and highly knowledgeable approach to acquiring or licensing intellectual property . . .” 10 U.S.C. § 2322 (b)(1).

2. Review proposed new Service and Agency unique IP requirements or provisions and provide recommendations as to whether they are consistent with the DFARS (including specifically negotiated license rights authorized by DFARS), whether an existing template would suffice, or whether the requirement warrants additional clearance through deviation or rulemaking procedures.
- c. Serve as an ombudsman for all IP disputes related to SCRs (e.g. SBIR IP disputes and whether Service and Agency unique IP clauses or provisions are contrary to the DFARS which results in an unauthorized circumvention of the rulemaking or deviation), by interacting with or assisting in interactions with contractors, including communications and negotiations with contractors on solicitations and awards and conducting or assisting with mediation if technical data delivered pursuant to a contract is incomplete or does not comply with the terms of agreements. See 10 USC 2322(b)(3)(E) and (F).

7. Treatment of Independent Research and Development (IR&D) versus Self-Funded Research and Development (SFR&D) for Intellectual Property (IP) rights determinations; IR&D risk correct for limited/restricted rights?

Tension Point

Should there be a distinction between IR&D, Bid and Proposal (B&P), manufacturing and production engineering (MP&E) and privately funded research and development (R&D)? Government panelists question whether the risk is apportioned appropriately. Industry panelists oppose any changes in the law and regulations that would treat IR&D and B&P as federal funding or otherwise expand the Government's rights in technical data.

Issue

Government panelists, and a Government witness, questioned whether IR&D and B&P costs should continue to be treated as “private expenses” for purposes of determining the Government’s rights in technical data. The Government witness noted that industry bears no risk when R&D is funded with federal funds since the costs are reimbursed as they are expended during contract execution.

Discussion

Companies seek to recover R&D costs in product pricing. A fundamental rule of establishing a pricing strategy in the commercial marketplace is that prices must cover both costs (such as R&D expenses) and profit. The objective is not to break even or to be “made whole” by recovering costs such as R&D investments, but to generate a return on investment (ROI) – profit.

Industry believes that unlike the commercial marketplace, when selling to the Government, they don’t have the freedom to set prices because in Government contracting costs and profit are regulated to ensure fair and reasonable prices for the products and services the Government buys with taxpayer dollars.

Applicable laws and regulations such as the Cost Accounting Standards (CAS)¹ and the Federal Acquisition Regulation (FAR) cost principles specify the manner and extent to which contractors can recover costs under U.S. Government contracts. Unique cost classifications such as IR&D, B&P, and Manufacturing and Production Engineering exist only because of the unique nature in which the Government regulates these costs under U.S. Government contracts. The CAS dictate

¹ See 41 U.S.C. 1501-1506, formerly 41 U.S.C. 422.

that contractors shall recover indirect costs such as IR&D and B&P through the General & Administrative (G&A) rate.

In Department of Defense (DoD) contracting, IR&D is funded and managed at the contractor's discretion, and some or all of the costs are later recovered in DoD contracts via G&A. While the method, and timing, of IR&D and B&P recovery differs from the commercial marketplace, the fact remains that all companies, in all markets and industries, seek to recover R&D costs in product pricing and sales.

IR&D is defined in FAR 31.205-18 as costs that consist of projects falling within the following four areas: (1) basic research, (2) applied research, (3) development, and (4) systems and other concept formulation studies. IR&D does not include: (1) costs of effort required in the performance of a contract or (2) technical effort expended in developing and preparing technical data specifically to support submitting a bid or proposal (i.e., B&P costs).²

B&P costs are defined in FAR 31.205-18 as the costs "incurred in preparing, submitting, and supporting bids and proposals (whether or not solicited) on potential Government or non-Government contracts." The term does not include the costs of effort sponsored by a grant or cooperative agreement, or required in the performance of a contract. B&P encompasses all effort in the preparation of a solicited or unsolicited proposal.

The Existing IR&D IP Policy Was Implemented to Incentivize Innovation

The issue of what constituted "private expense" development in DoD contracting had been debated since at least the 1960s. In the 1980s, Congress established the current statutory policy in 10 U.S.C. 2320 of treating IR&D and B&P as private expenses for purposes of determining the Government's IP rights, in order to incentivize contractors to invest in innovation.

The Government's view is that there is "no risk" in IR&D because all (or most) IR&D is recovered, and recovered quickly (cash flow benefit), due to the manner in which the CAS require indirect costs to be recovered while commercial companies do not recover IR&D costs unless the project is successful and sales are made.³ A government official suggested that the

² See FAR 31.205-18, Independent research and development and bid and proposal costs.

³ A contractor's annual IR&D budget is an estimated amount that is input into the calculation of Forward Pricing Rate Proposal (FPRP) G&A rates. The G&A rate is then submitted to Defense Contract Management Agency (DCMA) in the contractor's FPRP and the contractor and DCMA reach consensus on the FPRP. The rates contained in the FPRP (including G&A) are then utilized in both proposals and billings under U.S. Government contracts. Budgeted IR&D expenditures that resulted in the FPRP negotiation between the contractor and the U.S. Government are reimbursed to the contractor in accordance with the terms and conditions in a U.S. Government contract. Assuming the budgeted IR&D expenditures are close to the actual IR&D expenditures incurred by the contractor, the contractor is reimbursed for a certain portion of its estimated annual IR&D expenditure approximately 30 days after submitting a bill to the U.S. Government under a U.S. Government contract. Assuming FAR 52.232-25 is included in the contract, under the Prompt Payment Act an agency must make payment within the later of two

Government should obtain “government purpose rights” in the technical data pertaining to IR&D-funded technologies reimbursed under a government contract. Industry’s view is that there is risk in IR&D, as evidenced by the fact that contractors cannot indiscriminately invest in IR&D due to potential impacts to contractor rates.

Industry has also questioned how the Government would incentivize a contractor to invest IR&D dollars if the Government could subsequently (with Government Purpose Rights) provide the fruits of the contractor’s investments to competitors to compete against the contractor in production or sustainment contracts. The Government official’s proposal would also conflict with Small Business Innovation Research (SBIR) regulations if a small business were to invest its own IR&D dollars for work that derives from, extends or completes prior funded SBIR research. In this instance, the Government is prohibited by law from demanding rights in excess of its already granted SBIR data rights.

Government panelists also cited a 2014 Defense Business Board (DBB) report⁴ as support for their position that the law and regulations regarding treatment of IR&D and B&P for IP purposes should be changed. The DBB Task Force made several recommendations in its report, to include a recommendation to “rebalance policies on the ownership and rights to IP.” The Task Force reviewed three types of R&D (contracted R&D (CR&D), IR&D and SFR&D) and summarized them as follows:

events: (1) the 30th day after the designated billing office receives a property invoice from the contractor; or (2) the 30th day after Government acceptance of suppliers delivered or services performed. Payment is based on receipt of a “proper invoice and satisfactory contract performance.” See FAR 52.232-25(a)(1), Prompt Payment and FAR 32.905(a), Payment Documentation and Process.

⁴ Defense Business Board Report FY14-02, *Innovation: Attracting and Retaining the Best of the Private Sector*. <http://dbb.defense.gov/Portals/35/Documents/Reports/2014/DBB-FY14-02-Innovation%20report%20%28final%29.pdf>

Three Types of Research and Development (R&D)

Contracted R&D (CR&D) represents services for which the DoD contracts, as it does many kinds of services. In this case, the services constitute R&D services, with the focus being either general or specific. CR&D does not represent industry risk capital, nor should industry automatically have any kind of ownership of the intellectual property or technologies that result, unless such ownership is negotiated in the services contract.

Independent R&D (IR&D) represents expenditures that industry makes in undertaking R&D of its choosing, but with government funds. Specifically, the funds industry expends for this kind of research are bundled into its general and administrative or overhead cost pools and subsequently billed to the government on an established billing cycle. In the case of IR&D, the expenditures do not constitute industry risk capital, but do represent industry resource allocation decisions. Industry's claim that IR&D represents its own risk capital is in our view, wrong. Ownership of the intellectual property or technology that results from IR&D needs to be clarified. It would be appropriate for such ownership, or the rights to use the technology developed, to be shared between government and industry.

Self-funded R&D (SFR&D) is characteristic of the commercial industry, and also occurs (to a much lesser extent) within the DIB. It represents the expenditure of industry's own capital into R&D or other similar investment areas. In this case, the funds being invested are not recovered by bi-monthly, monthly, or progress payments charges to the government. This capital is truly risk capital by industry; ownership of the results of such investment, including intellectual property, should reside 100% with industry.

Industry panelists disagree with the DBB's summary of, and recommendations for, IR&D. First, IR&D is not equivalent to direct government funding. IR&D exists as a unique cost classification only because the defense industry is a regulated industry. If the Government did not regulate costs or profits, and the DoD acquired products and services through the negotiation of prices similar to the commercial marketplace, then the DoD would have no visibility into contractor R&D costs and profit margins, and there would be no question whether defense contractor R&D expenses were industry risk capital. The reality is that in this regulated environment, where the Government regulates both costs and profit, the only practical way for traditional defense contractors to ensure that they recoup R&D investments in the sale of products or services to the DoD is through IR&D recovery. The CAS and the FAR do not provide any another effective mechanisms to recover previously expended R&D costs such as SFR&D.

Second, R&D risks in the commercial and defense markets are indeed different. There are variables that contribute to IR&D risk, many of which are beyond defense contractors' control: the technology may not "prove up"; the DoD may cancel planned programs, significantly delay new program starts, or buy fewer units than originally intended – all of which may undermine the projected ROI in the contractor's original investment decision; Congress may not fund a new

program, or the procurement of additional lots; and finally, a contractor may not win new business to which IR&D projects relate. If a contractor were to dramatically increase its IR&D expenditures without consideration of these business risks, and didn't capture sufficient new business, then the contractor's rates would increase, thus making it difficult for the contractor to compete on price in future DoD procurements.

As the DBB Task Force pointed out in its report, profit is risk-calculated and plays a role in companies' willingness to invest in innovation.

In comparison, U.S. defense contractors generally develop their products for sale to one customer, the U.S. Government, which may buy a few hundred units of a product. Additional sales may or may not be possible with the addition of foreign military sales. Most SFR&D performed by the defense industrial base is performed by companies with hybrid business models, which have both commercial and defense divisions. Traditional defense contractors, which do not have commercial portfolios, do not have the flexibility to offset SFR&D risks through commercial sales. They generally cannot justify the risks associated with SFR&D because they would have very limited opportunities to recover their investments. SFR&D occurs at a much lower rate in the defense industry because traditional defense contractors generally cannot justify the risks of SFR&D investments with projected sales and profit margins.

The Defense Federal Acquisition Regulation Supplement (DFARS) recognizes the unique differences between IR&D and the majority of SFR&D performed in the defense industrial base. The DFARS prescribes different policies for acquiring commercial and noncommercial technical data, with the DoD generally acquiring only the commercial technical data that is customarily provided in the commercial marketplace.

IP Protection as an Incentive to Innovate

While the DBB Task Force discussed profit as an incentive to invest in its report, it did not discuss the extent to which IP protection incentivizes IR&D investment nor cash flow impacts. Further, the Task Force did not analyze the extent to which modifying the IP framework for IR&D/B&P may impact defense contractors' willingness to invest in IR&D. Industry believes that traditional defense contractors generally cannot justify significant SFR&D investments with existing profit margins, and if the Government were to change its IR&D IP policy, it is unlikely that traditional defense contractors would shift the bulk of their IR&D expenditures to SFR&D. Instead, contractors may forego certain investments altogether. Thus, from the industry's perspective, significant questions are left unanswered in the DBB report –

- 1) If the Government removes contractors' ability to secure a competitive advantage by protecting the IP pertaining to IR&D-funded technologies, then how will the Government incentivize contractors to invest in IR&D?

- 2) If the Government changes its IR&D IP policy, would overall IR&D expenditures in the defense industrial base decline at a time when the U.S. Government is concerned about threats to U.S. military superiority?
- 3) How would changes to the existing IR&D IP policy impact the overall health of the defense industrial base? Would companies exit the market altogether?
- 4) Is the DoD prepared to offset a potential decline in contractor IR&D investments through an increase in CR&D?

Government panelists recommend the following statutory changes to 10 U.S.C. 2320(a)(3):

The Secretary of Defense shall define the terms “developed”, “exclusively with Federal funds”, and “exclusively at private expense” in regulations prescribed under paragraph (1). In defining such terms, the Secretary shall specify the manner in which indirect costs shall be treated and shall define conditions and criteria that balance the legitimate interests of the United States and of a contractor or subcontractor regarding the extent to which specify that amounts spent for independent research and development and bid and proposal costs shall ~~not~~ be considered to be exclusively with Federal funds, exclusively at private expense, or in part with Federal funds and in part at private expense, for the purposes of the definitions under this paragraph.

Industry panelists do not agree with the Government panelists’ recommendation since there is no data to back up the impact of the recommended change.

Recommendation

The Panel recommends prior to any changes to 10 U.S.C. 2320(a)(3) that further study and analyses be accomplished to assess the potential impact to overall IR&D and MP&E spending in the defense industrial base. The Panel recommends an independent study to analyze and assess incentives and risks for IR&D and MP&E investment and the role of technical data rights in investment decisions:

“SEC. XXX. Independent Study of Incentives and Risks for IR&D, B&P and MP&E Investments.—

(a) Requirement for Study.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall enter into a contract with an independent research entity described in paragraph (b) to carry out a comprehensive study of incentives and risks for independent

research and development (IR&D), bid and proposal (B&P) and manufacturing and production engineering (MP&E) investment, including—

- (1) the circumstances under which development costs may be classified as IR&D, B&P, MP&E or other indirect costs under the Cost Accounting Standards and the Federal Acquisition Regulation;
- (2) treatment of IR&D, B&P, MP&E and other indirect costs for purposes of determining rights in technical data;
- (3) the extent to which profit margins, cash flow and technical data rights affect investment decisions,
- (4) a comparison of the commercial and defense markets
- (5) an assessment of recommendations for statutory or regulatory changes, to include consideration of:
 - (A) the above noted statutory changes recommended by the Government panelists or
 - (B) an alternative where costs charged as IR&D and B&P, MP&E and other indirect costs are treated as private expense for a limited period of time after they are incurred and as Government funding thereafter, or
 - (C) other alternatives, to include whether no changes are warranted;
- (6) treatment of IRD, B&P, MP&E, and other indirect costs used for furthering SBIR developed technology; and
- (7) any other areas the Secretary deems important.

(b) Independent Research Entity.—The entity described in this subsection is an independent research entity that is a not-for-profit entity or a federally funded research and development center with appropriate expertise and analytical capability.

(c) Independent Research Entity needs to reach out to government and industry.

(d) Reports.—

- (1) To Secretary.—Not later than twelve months after the date of the enactment of this Act, the independent research entity shall provide to the Secretary a report containing—
 - (A) the results of the study required by paragraph (a); and
 - (B) such recommendations as the independent research entity considers to be appropriate.
- (2) To Congress.—Not later than 60 days after receipt of the report under subparagraph (1), the Secretary of Defense shall submit such report, together with any additional views or recommendations of the Secretary, to the congressional defense committees.”

8. Is Source of Funding the Best way to Determine Rights to Technical Data?

Tension Point

Does the Department of Defense's (DoD) current approach, determining rights to technical data and software based primarily on source of development funding, meet its needs while providing industry a predictable business model at a reasonable cost to the taxpayer? Are there other alternatives worthy of consideration?

Issue

Because of its unique mission and sustainment needs, the DoD requires/seeks more access to technical data and software than other consumers. Anecdotal evidence indicates that this may have caused leading technology firms to avoid the defense business for fear that, in providing the DoD such access, their competitive edge might be compromised. This effect reduces the size of the defense industrial base and puts one DoD interest in conflict with another.

At the same time, the DoD invests in myriad technologies to secure its own competitive and innovative advantage and encourages industry to do the same. The DoD has an interest in providing industry with a predictable business model and incentivizing private investment in research and development (R&D). DoD also is interested in receiving a reliable return for its investment. The challenge is to balance these competing interests at a reasonable cost to the taxpayer.

Discussion

Current Policy (Defense Federal Acquisition Regulation Supplement (DFARS) Part 227):

With some exceptions, the DFARS allocates Government rights in noncommercial technical data and software **(1) according to the funding contributions of the parties and (2) specifically negotiated license rights.** The DFARS outlines separate policies for the acquisition of commercial technical data and computer software.

1. Source of Funding – Noncommercial:

- (a) *Unlimited rights* – The Government obtains unlimited rights in technical data for items, components, or processes **developed exclusively with Government funds**
- (b) *Government purpose rights (GPR)* – The Government obtains rights in technical data pertaining to items, components, or processes developed with **mixed funding** (typically converts to unlimited rights after 5 years) under DoD contracts, unless the portions developed exclusively at private expense are segregated from the portions developed with Government funds.

As part of Section 809 of the fiscal year (FY) 2017 National Defense Authorization Act (NDAA), this default rule was changed to one that requires special negotiation.

- (c) *Limited rights/Restricted rights* – The Government has restricted rights to data, if items, components, or processes were **developed exclusively at private expense**.
- (d) *Segregability* – The DFARS applies a segregability approach when making funding determinations. Portions of an item or software developed exclusively at private expense are segregated from the portions developed with Government funds.

Strength: The strength of the Source of Funding method is that traditional defense contractors and DoD employees understand the concept that rights go with funding, partly because there is an inherent justice in having the party who paid for the development reap the rewards. Industry also benefits because industry still owns and can patent the “technological breakthroughs” developed by research funded entirely by the DoD. Industry also obtains a first mover advantage in the market and acquires human capital that is not easily replicated by merely providing the data and software to a potential competing source. These advantages allow contractors to strengthen their market positions and to increase their future profits even when the R&D costs are borne entirely by the DoD.

Weakness: The weakness of the Source of Funding method is its implementation. There is very little agreement between the DoD and industry on how the method applies in practice. Even when there is agreement, policing the implementing concepts of “mixed funding,” “developed,” “government funds,” “private expense,” and “segregability” are very burdensome. It not only requires recording and maintaining information that is not ordinarily done in the course of business, but the terms are unique to DoD and federal procurement and leave much room for interpretation. All of these make the source of funding paradigm extremely complicated to apply to commercial items. At the same time, to prevent downstream mixed funding risks, contractors often default to the “doctrine of segregability” and redirect critical program engineering resources away from technical tasks to administrative tasks (e.g., portion-marking technical data and annotating source code header files).

2. Specifically Negotiated License Rights (SNLR):

When using this approach, the parties agree to modify the standard license rights granted to the Government (e.g., GPR). It is useful in any number of circumstances where the default license rights do not meet the Government’s particular needs. At times, the DoD includes a SNLR provision in its solicitations but industry believes this is underutilized. Contractors may also seek to negotiate SNLR provisions when they have invested private funds to develop a technology that will be modified with DoD funds, or, where they have enhanced or upgraded technologies originally developed in part with Government funds.

In the event either party requests SNLR and as feasible or practical, the parties should consider this approach, particularly if it better supports the long-term sustainment requirements of the warfighter. Because this approach requires considerable time, more experienced Government

staff, and more in-depth analysis, it may be more appropriate for the larger dollar value DoD programs, such as Acquisition Category (ACAT) I acquisition programs.

Strength: The strength of the negotiated license rights is its flexibility. Industry's view is that SNLR may obviate instances of contractor reliance on the "doctrine of segregability," resulting in more practically usable data/rights solutions for the DoD.

Weakness: The primary weakness of this approach, is that it requires DoD program managers to identify life-cycle requirements for technical data and software in the very early acquisition phases, when the DoD has leverage to negotiate but limited knowledge of its future needs. If sustainment needs change after contract award, the DoD may not have sufficient leverage to negotiate for additional rights. Also, when every program negotiates its own terms, industry is deprived of a predictable business model on which it can make future investments. Finally, if practiced as a default rule, SNLR could undermine other DoD interests.

Some of the alternative approaches discussed below, such as temporal or event-based licensing and the negotiation of priced contract options, can be used to mitigate the impacts associated with sustainment planning changes.

Alternatives to Current Policy:

1. Needs-Based Acquisition of Technical Data Rights: This is a variant of the SNLR approach, where the DoD's acquisition programs purchase data and software license rights only as it is needed. Another variant of this approach is one where the DoD acquires a certain amount of data and software, based on some presumptive need, such as spare-parts procurements or depot-level maintenance. Priced-options can be used in this approach, but in all variants, they require DoD personnel to forecast their needs with a high degree of accuracy.

Strength: It is easier to negotiate and purchase data and software when specific needs are known, so long as those needs can be traced to particular data and software end items and the market dynamics facilitate the exchange.

Weakness: DoD acquisition personnel rarely have perfect knowledge of life-cycle needs in the early phases of the program when negotiation leverage exists. When the knowledge exists, however, the market dynamics are not favorable to the DoD, and coming to agreement on a fair and reasonable price for the data and software is very difficult, if not impossible, unless the DoD is willing to pay a very high price. In some cases, contractors are unwilling to deliver the data or software at any price if doing so threatens their business model and future profits.

2. Temporal-Based or Event-Based Standards: This is a variation on how rights in data and software could be allocated through the DFARS or through SNLR. Rather than establish a unique framework, this approach relies on the timing of when readily understood criteria are met to allocate rights in data and software. The patent clauses provide an example of such an approach. A variant of this approach could establish a basic scheme that allows rights to become more permissive over time, thereby granting a limited time to industry to recoup investment costs.

Strength: By employing objective and readily observed criteria, rights could be allocated according to readily observable events relating to a contract's performance period. Some contract administration would be required, but preferably less than is required by the current rules. When the criteria are more objective, the potential for disagreement between the DoD and industry is reduced.

Weakness: Establishing criteria that are not overly intrusive or require burdensome administration may not be straightforward.

3. **Copyright-Based Standards:** Copyright standards, as opposed to the patent-like standards embedded in the DFARS, could be adapted to allocate rights in data and software given that both are forms of copyrightable works. Most open source licenses operate from copyright-based standards and principles.

Strength: Copyright standards may be easier to administer because they come with a well-developed, highly nuanced, and well-understood body of statutory and case law. Relying on this background, it may be easier to assess DoD needs using agreed to definitions rather than invoke lesser understood statutory and regulatory concepts that are not readily understood.

Weakness: Computer databases are typically not protected under U.S. copyright law, and thus would need separate coverage, or, like the current rules, no coverage at all. Industry panel members are concerned about the protection for industry trade secrets provided by 18 U.S.C. 1905 and the DFARS. According to industry panel members, the DoD's past attempt to protect industry trade secrets expressly was not totally successful, so the DoD must assess whether its data and software requirements are likely to implicate a contractor's trade secret interests. This is another area of current disagreement between the DoD and industry.

4. **Directed Licensing Approaches:** This approach is one where the DoD contracts for the data owner to license technical data, software, and possibly provide technical assistance to establish alternative sources for supply, service, or even production. The data owner is paid a fee for the services (if required) and a royalty for providing the data and software to the alternative source. Reasonable and non-discriminatory (RAND) licensing schemes, which are often used by standards-setting organizations, are comparable to a directed license.

Strength: In a directed licensing scenario, a contractor remains in control of the data and software while the DoD retains the benefits of having an alternative source without having to establish one directly. Directed licensing terms, much like RAND licensing schemes, are typically easier to establish early in the life cycle when the DoD desires flexibility and contractors are forming a business model. Directed licensing, which may be prohibited by statute, is not prevalent in DoD acquisition. RAND licensing, on the other hand, is very prevalent in the commercial marketplace and readily understood by commercial firms.

Weakness: The terms of a directed license arrangement must be negotiated while market forces provide leverage (i.e., prior to contract award). This includes the royalty rate for any required

data or software. Additional fees for services could be addressed on a case-by-case basis, but allowable costs for such services are easier to evaluate.

Recommendations

The panel recommends no change to 10 U.S.C. 2320 or 10 U.S.C. 2321.

The panel does recommend some regulatory changes, identified below:

- 1) We recommend “Source of Funding” remain the default position until a better alternative that is mutually acceptable to Government and industry is identified.
- 2) We recommend that the DoD and industry recognize and employ, as appropriate, the various alternatives addressed here.
- 3) The DoD should promulgate guidance and templates for the alternative approaches that can be followed, as circumstances dictate.
- 4) We recommend language be included in the Request for Proposal for ACAT I acquisition programs to notify offerors that when they propose mixed funding technology, they have the option to propose SNLR.
- 5) We recommend that in the event long-term sustainment for major systems is considered, the parties should actively discuss SNLR.

9. Commercial vs. Noncommercial Items

Tension Point

Data rights for commercial items are not always determined based on the parties' legitimate interests.

Issue

The Government's license rights for noncommercial items are generally determined according to whether the Government contributed to the item's development. For commercial items, the DoD has tailored its data acquisition policies and rules to support the preferences of 10 U.S.C. 2377. Specifically, Defense Federal Acquisition Regulation Supplement (DFARS) 227.7102 states that DoD shall acquire only the technical data customarily provided to the public with a commercial item or process, except technical data that are: (1) form, fit, function; (2) required for repair or maintenance when such data is not customarily provided to commercial users or is not sufficient for military purposes; or (3) data that describes modifications made at Government expense to commercial items.

It is this latter scenario where the current data clauses and acquisition policies could be improved. The DFARS commercial technical data clause (252.227-7015), as it currently stands, only partially recognizes that greater rights should be afforded to the Government when based on a prior contract, which may include those where all or a portion of the commercial item was "developed" with government support. Also, when modifications are being made, neither the policies nor the rules provide much guidance as to whether the modifications being made rise to the level that they could impact the Government's intellectual property rights. Also problematic, from a policy perspective, is that the DFARS commercial data acquisition policies do not plainly recognize that the Government may already have rights in a commercial item because, prior to it becoming a commercial item, the Government may have paid for all or part of the item's development.

Discussion

It is generally accepted in the DoD that the buyer is entitled to greater intellectual property rights when funding technological development. The implementing regulations apply the current statutory funding concept regardless of whether the item/process is commercial or noncommercial. According to the statutes and implementing regulatory scheme, the parties' relative investments should be recognized, and the rights should be allocated accordingly, to allow a reasonable return on the parties' respective investments. There is a view in industry that the legislative record is unclear as to whether, and to what extent, Congress has intended the statutes to apply to commercial items, particularly in the case of commercial items modified with government funds to meet government-unique requirements.

Issues arise when the DoD has funded: (1) the “development” of some portion of the commercial item; (2) modifications to commercial items or (3) all or some portion of the development of the underlying item or process, which at some later time became a commercial item (with/without additional private investment by the contractor).

A significant shortcoming in the current procurement scheme resides in how the commercial item clause accounts for Government investments. Specifically, the commercial item clause (DFARS 252.227-7015) only partially recognizes the potential for prior or on-going Government investments and instead allocates rights based on a presumption that the item was funded exclusively at private expense. When the Government is funding on-going modifications and improvements, the current clause relies on the non-commercial clause to protect the Government’s investments, but only provides general guidance as to how the two clauses apply. Thus, in its solicitations and ensuing contracts, the Government has also been including the noncommercial clause (DFARS 252.227-7013, Rights in Technical Data—Noncommercial Items), to allocate rights in the portions of the commercial item “developed” with Government funds.

This approach is problematic for industry in that, according to their view, it may give the false impression that the commercial items have somehow been converted at least partially to noncommercial items. Industry has also expressed concerns that applying the noncommercial clauses to commercial items undermines the benefits and protections afforded to such items, which are meant to protect industry’s commercial interests. The Government, on the other hand, has maintained that whether an item is commercial or noncommercial is not affected by which data rights clause applies, and that the data rights clause is only meant to preserve the Government’s interests. Thus, the concern for both Government and industry is that, regardless of which clauses are used, the legitimate interests of both sides are respected.

Some industry representatives challenged the current practice as being inconsistent with 10 U.S.C. 2377 and the definition of “commercial item” at Federal Acquisition Regulation 2.101. Industry’s position is that even though a modified item is unique to a particular military application and not sold in the commercial market, it should still be subject to a commercial license if it meets the commercial item definition. To apply a noncommercial data clause to a commercial item, in their view, undermines the statutory preferences found in 10 U.S.C. 2377. In other words, applying a non-commercial data clause to protect the Government investments in a commercial item may discourage commercial vendors from selling commercial items to the Government.

DoD representatives have an alternate view that accounts for more than just the definition of a commercial item. DoD representatives also recognize that market realities should be accounted for when applying the commercial item policies and rules. When an item is unique to military applications, the DoD is the market—even if the item technically qualifies as being “commercial.” Their view is that the DoD should not subject itself to a commercial license in such situations without adequate market research to show the license is reasonable. Rather, in such circumstances, contracting officers should account for the market realities, in part by using contract clauses that allow for the DoD to capitalize on its buying power when it exists and to

protect its investments. For data acquisition, those interests are embodied in the non-commercial clauses.

Although the current regulations try to strike a balance by requiring the use of both clauses in certain circumstances, the implementing guidance relies exclusively on the Government knowing where, when, and how Government funding has occurred in relation to an item's development. The Government does not always have this information, and when relying exclusively on the commercial clause, the Government's investments are unlikely to be protected as described above. Thus, the state of the commercial clause requires the non-commercial clause to be included, which causes the concerns described above.

Moreover, whether an item qualifies as commercial or non-commercial, and which clause should apply, is not expressly based on market realities, which frustrates the DoD's acquisition objectives related to capitalizing on its buying power and protecting its investments. Though some of these issues could be alleviated through negotiations, the regulations do not provide instructions on how to negotiate for different rights for such changed items; nor do they create an incentive for vendors to negotiate for licenses prior to modifying a commercial item. Instead, both parties are left in a muddle, and neither is content.

Recommendations

The Panel does not recommend any changes to 10 U.S.C 2320 or 2321.

We recommend regulatory changes to the DFARS, as follows:

- 1) **Add the following paragraph at the end of DFARS 227.7102-1, Policy:**
(d) When the technical information or the technical data customarily provided to commercial users is not sufficient for the DoD and military purposes, the Government should negotiate with the commercial item/process owner to obtain the data required for its purposes.
- 2) **Amend DFARS 227.7102-2(b) as follows:**
If additional rights are needed, contracting activities should negotiate with the contractor to obtain such rights and the additional rights should be specified in the contract. Where the Government identifies a need for long term sustainment of the commercial item, such negotiations should include provisions to allow the Government or a third party to maintain the data when the commercial item owner is no longer providing support for the commercial item. Before entering into such negotiations, contracting officers should investigate the development of the commercial item and whether greater rights have already been afforded in a prior contract.
- 3) **Revise DFARS 252.227-7015, Technical Data—Commercial Items** to add a paragraph or create an Alternate version
Revise the Commercial Item clause, 252.227-7015, or create an “Alternate” version of the clause, and associated prescription and flow-down language, as appropriate. The revised

clause or alternate should recognize the funding contribution of the Government and allocate rights accordingly. This could eliminate the need to include both commercial and noncommercial clauses when commercial items are developed with contributions from Government funds. It would thus have the benefit of using the commercial clause when the item is commercial, rather than creating the appearance of treating a commercial item as noncommercial by using the noncommercial clause.

4) Add a new paragraph (d) to DFARS 227.7202-1, Policy as follows:

(d) When a commercial computer software license does not meet user needs, the Government should negotiate with the software owner to acquire additional rights. Where the Government has a need for long term sustainment of the commercial software, negotiations should include a software transition plan and related contractual provisions to allow transition from the Original Equipment Manufacturer to the Government or third party to maintain the software, when the commercial software owner is no longer providing support for the commercial software. Before entering into such negotiations, contracting officers should investigate the development of the commercial item and whether greater rights have already been afforded in a prior contract.

5) Update Policy and Contract Clauses to account for the Government's prior rights.

Revise and update current contract clauses and governing policies to clarify that the DoD will not be divested of pre-existing rights in data or software pertaining to a non-commercial item if the item is reclassified as a commercial item. Include better guidance for distinguishing when a modification to a commercial item warrants granting greater intellectual property rights to the Government.

10. Commercial Software License versus Government-unique Requirements

Tension Point

Commercial software licenses have terms which the Government believes need to be changed to meet procurement objectives.

Issue

The Panel received information about issues relating to commercial software licenses used by the Government. The normal commercial practice for licensing software to an end user is for the software owner to attach a contract to its software, which binds any end user of that software license - (End User License Agreement (EULA)). Distribution entities, such as prime contractors, who are merely distributing the software will have a separate license from the distribution or value added reseller license which allows these distribution entities to provide the software to the end user. Each EULA is drafted uniquely to meet a particular risk profile for the software, usually reflecting the amount paid by the end user for a copy, the size of the software owner, and the amount of customization the software owner allows.

Industry representatives note that, while some software owners are willing to negotiate their EULAs to meet a particular user's needs, other owners would prefer not to license the software at all or make it difficult to negotiate a EULA.

Government end users have specific procurement laws and statutes which can conflict with these EULAs. This results in Government users being required to review each provided EULA to ensure consistency with laws and needs. Government representatives have maintained that EULAs do need to be adjusted in many cases to meet these needs, but there is no consistency on which EULA clauses should be changed due to conflicts with law or with agency needs for a particular procurement. Further, negotiation of each EULA for each procurement is a drain on Government resources, and there is a need to ensure any negotiated EULA is preserved.

Industry representatives have noted that, in order to meet this need, Government end users are increasingly attempting to mandate changes to EULAs. As examples, Industry representatives point to the use of H clauses to require specific standard EULA clauses and Federal Acquisition Regulation (FAR) clause, FAR 52.232-39, which was created to address a potential Antideficiency Act issue. Industry representatives acknowledged that EULAs may need to be changed for specific issues, but any such change alters the risk profile for each particular EULA, and each change (if made standard) is contrary to the requirements of 10 U.S.C. 2377 and similar statutes requiring the use of commercial terms and conditions to the extent such requirements are not required by law. Industry representatives have asserted that the use of H clauses and FAR

clauses to change EULAs is inappropriate since these clauses are only applied to the prime contract, and are not directly negotiated with the software owner. They may become inappropriate flowdowns causing risks to the supply base and prime contract resources, if they attempt to negotiate the Government's terms.

The Panel also received information about issues relating to Foreign Military Sales (FMS). Under a FMS, the Government is not the end user and should only have a distribution right. Therefore, the Government should not be evaluating EULAs or suggesting changes to EULAs except as directed by the FMS customer.

The Panel further received comments from Government personnel that current regulations do not account for storage of commercial software licenses. Since commercial software licenses are not issued as regulations, it is possible that such licenses would be lost. Since many commercial software licenses are for an indefinite term license, the existing records retention regulations do not account for the necessary protections of commercial software licenses.

Recommendation

The Panel does not recommend any changes to 10 U.S.C. 2320 or 2321.

The Panel recommends that the following changes be made to the DFARS:

DFARS 227.7202-3, Rights in commercial computer software or commercial computer software documentation.

(a) The Government shall have only the rights specified in the license under which the commercial computer software or commercial computer software documentation was obtained, including where the Government is an end user for the software or is a distributor of such software to a third party under a Foreign Military Sales under DFARS 225.73. To the maximum extent possible, the Government should use any existing terms and conditions already negotiated between the Government and the software owner. The contracting officer shall ensure that agency record retention rules preserve such license for the applicable term of the license

(b) If the Government has a need for rights not conveyed under the license customarily provided by the software owner to the public, the Government must negotiate with the contractor software owner to determine if there are acceptable terms for transferring such rights. The specific rights granted to the Government shall be enumerated in the contract license agreement or an addendum thereto.

(c) Where the Government is evaluating a potential change to the license customarily provided to the public, the Government will consider the risk to the software owner in making such change, consult with agency intellectual property counsel, and propose the change which is least impactful to the software owner, while consistent with Government laws and regulations and avoiding an impact to pricing in the contract under which the software is provided to the Government. The Government will directly negotiate such potential changes with the software owner, and the software owner will provide any changes to the software owner's license to the contractor.

DFARS 227.7202-4, Contract clause.

A specific contract clause governing the Government's rights in commercial computer software or commercial computer software documentation is not prescribed. As required by 227.7202-3, the Government's rights to use, modify, reproduce, release, perform, display, or disclose computer software or computer software documentation shall be identified in a license agreement. Any contract provision which mandates a change to a commercial software license is expressly prohibited except as mandated for clauses in the FAR or DFARS.

DFARS 227.7102-4, Contract clauses.

(d) Where the Government's acquisition of the technical data also includes the need to provide the technical data to a third party under a Foreign Military Sales under DFARS 225.73, the above clauses may not provide an appropriate end user license to that third party. The Government will obtain an end user license from the technical data owner for the third party which will provide restrictions consistent with commercial practices and allow the Government to distribute the technical data to the third party end user. The contracting officer shall ensure that agency record retention rules preserve such end user licenses for the applicable term of the license.

DFARS 227.7103-6, Contract clauses.

(f) Where the Government's acquisition of the technical data also includes the need to provide the technical data to a third party under a Foreign Military Sales under DFARS 225.73, the above clauses may not provide an appropriate end user license to that third party. The Government will obtain an end user license from the technical data owner for the third party which will provide restrictions consistent with commercial practices and allow the Government to distribute the technical data to the third party end user. The contracting officer shall ensure that agency record retention rules preserve such end user licenses for the applicable term of the license.

DFARS 227.7203-6, Contract clauses.

(g) Where the Government's acquisition of the computer software or computer software documentation also includes the need to provide the technical data to a third party under a Foreign Military Sales under DFARS 225.73, the above clauses may not provide an appropriate end user license to that third party. The Government will obtain an end user license from the computer software or computer software documentation owner for the third party which will provide restrictions consistent with commercial practices and allow the Government to distribute the computer software or computer software documentation to the third party end user. The contracting officer shall ensure that agency record retention rules preserve such end user licenses for the applicable term of the license.

11. Authorized release and use of limited rights technical data

Tension Point

Recent legislation (and proposed legislation) creating additional grounds for authorized release of limited rights technical data have not all clearly been tied to a defined use.

Issue

10 U.S.C. 2320(a)(2)(D) has long authorized the release of limited rights technical data to, and use of such data by, persons outside the Government in two cases: (1) for emergency repair and overhaul, or (2) for evaluational or informational purposes by a foreign government. The latter does not apply to detailed manufacturing or process data, and the Department of Defense (DoD) regulations implementing the former require that “[t]he Government shall require a recipient of limited rights data for emergency repair or overhaul to destroy the data and all copies in its possession promptly following completion of the emergency repair/overhaul and to notify the Contractor that the data have been destroyed.”¹ In either case, the release or use statutorily must be subject to a prohibition on further release, disclosure, or use by the recipient.²

The Fiscal Year (FY) 2012 National Defense Authorization Act (NDAA) added a third case for which limited rights technical data could be released or used: when 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.³ The House version of the FY2017 NDAA proposed to remove this segregation/reintegration case and replace it with yet another limited rights exception: a release, disclosure, or use of technical data pertaining to an interface between an item or process and other items or processes.⁴ The final version of the FY2017 NDAA, which was released after this tension point was captured, combines the two previous statutory approaches. Namely, the following limited rights exception replaces the FY2012 version: is a release, disclosure, or use of technical data pertaining to an interface between an item or process and other items or processes 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.⁵

Throughout, there has been a lot of uncertainty and concern expressed about what limited rights data is, in fact, subject to this authorized release. This is especially important because, unlike the

¹ DFARS 252.227-7013(b)(3)(ii).

² 10 USC 2320(a)(2)(D)(ii).

³ Section 815(a)(1)(A)

⁴ Section 1705(b)(3)

⁵ Section 809(b)(3)

unusual occurrence of an emergency (which, by definition, is both unexpected and urgent), the intent appears to be more frequent releases/uses that likely would result in a new or alternative item or process (or new combination of items or processes) that could either incorporate or be derived from the original interface or ‘segregation or reintegration’ data and supplant the original item or process. Therefore, industry has expressed great concerns that such release and use would circumvent the protections applicable to the original technology and infringe the trade secrets inherent in the interface or ‘segregation or reintegration’ data.

In the case of the final FY2012 and FY2017 versions, there is uncertainty as to how deep within a privately funded item or process (i.e., inside the black box) the segregation might occur or interface might reside, and as to the relationship between the interface and the item or process being segregated or reintegrated.

Subsequent to the release of the House bill but before the final FY2017 NDAA, the DoD published a proposed rule⁶ implementing the segregation/reintegration provisions of the FY2012 NDAA discussed above. That proposed rule defined segregation or reintegration data to be “at any practical level, including down to the lowest practicable segregable level,” which correlates to the test for determining private expense development.⁷ This definition further fanned industry’s concerns about the inevitable exposure of trade secrets inherent in the ‘segregation or reintegration data’ residing at low levels within the items or processes (or software, by virtue of the proposed rule’s explicit extension thereto) that it has developed at private expense. While the use of the term “interface” in the FY2017 NDAA would seemingly limit the level at which the Government is obtaining data (e.g., at a boundary between items or software modules actually purchased and upgraded by the Government, as opposed to supposed interfaces lying within the component or software module), industry remains concerned that any implementing regulations would not respect such boundaries and instead define the term “interface” to achieve a similar result to what was proposed in Defense Federal Acquisition Regulation Supplement (DFARS) Case 2012-D022.

In many cases, these industry concerns will prevent companies from providing DoD access to innovative products, technologies, and processes developed for commercial use. These concerns also are unlikely to encourage (and, conversely, are likely to discourage) private sector investment in new products, technologies, and processes relevant to the missions of the DoD.

⁶ FR 39482 (DFARS case 2012-D022)

⁷ As defined in DFARS 252.227-7013(a)(8) and 252.227-7014(a)(8)

Recommendation

The Panel recommends a statutory change to 10 U.S.C 2320 as follows: In order to avoid the unintended consequences, segregation or reintegration data should be statutorily limited to the end item level or higher, i.e., 2320(a)(2)(D)(i)(II) should be amended as follows:

is a release, disclosure, or use of technical data pertaining to an interface between the an item or process and other items or processes necessary for the segregation of the 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

This approach clarifies that the interface in question and the segregation/reintegration activities pertain to the item or process that was developed exclusively at private expense and for which the data rights of the Government have been restricted pursuant to section 2320(a)(2)(B). Interfaces within that item or process are not subject to 2320(a)(2)(D)(i)(II).

This approach also aligns well with the doctrine of segregability. In a case where a contractor has employed the doctrine in order to restricted the rights of the Government in data pertaining to select, segregable sub-item(s) or sub-process(es), then it is the interfaces within those select sub-items or sub-processes that are not reachable via 2320(a)(2)(D)(i)(II). However, data pertaining to the interfaces between those select sub-items or sub-processes and other sub-items or sub-processes may well be subject to 2320(a)(2)(D)(i)(II) in order to conduct segregatation/reintegration activities on those select sub-items or sub-processes.

The panel recommends the following changes to the implementing regulations to:

- 1) create separate definitions for interface data necessary for segregation and reintegration based upon whether this data pertains to items or processes and whether this data is technical data or computer software, and in terminology which is understood by each industry;
- 2) require that, to the maximum extent practicable, when it is determined that the government may require interface data necessary for segregation and reintegration, the government and contractor will enter into negotiations, prior to contract award, to specify by mutual agreement the required nature and character of that data that will be subject to a delivery requirement;
- 3) in cases where the parties have not agreed prior to award on the interface data in question, provide the owner of the segregation/reintegration interface data an express pre-disclosure right to redact technical data or computer software to exclude any content not necessary;
- 4) require contractor to whom the release will be made, prior to release, be subject to conditions and restrictions similar to those that apply to covered government support

- contractors so that the original contractor can understand how its competitor has complied; and
- 5) provide the original contractor with mechanisms to ensure that the competitor has complied with applicable Limited Rights, Commercial Rights, or Restricted Rights licenses.

Regarding item #4, the contractor to whom the release was made could also be required to sign a non-disclosure agreement with the Contractor to establish the boundaries of use of the Limited Rights interface data, including prohibitions on using the data for any other purpose or for the benefit on any party other than the Government, and destroying or returning the data to the Government at the completion of work.

12. Are Existing Rights Sufficient for Maintenance and Sustainment?

Tension Point

The Government and industry have different views regarding the form of data and data rights to fulfil maintenance and sustainment requirements for equipment and software.

Discussion

Life-Cycle Management and Product Support

10 U.S.C. 2337, Life-Cycle Management and Product Support, states:

“(a) Guidance on Life Cycle Management. The Secretary of Defense shall issue and maintain comprehensive guidance on life-cycle management and the development and implementation of product support strategies for major weapon systems. The guidance issued pursuant to this subsection shall—

- (1) Maximize competition and make the best possible use of available Department of Defense and industry resources at the system, subsystem, and component levels; and
- (2) Maximize value to the Department of Defense by providing the best possible product support outcomes at the lowest operations and support cost.”

10 U.S.C. 2337 defines “product support” as

“the package of support functions required to field and maintain the readiness and operational capability of major weapon systems, subsystems, and components, including all functions related to weapon system readiness.”

The Department of Defense (DoD) Integrated Product Support Element Guidebook (2011) identifies the Integrated Product Support Elements (IPSE) (basically, the elements making up product support):

- (a) Design Interface
- (b) Sustaining Engineering
- (c) Supply Support
- (d) Maintenance Planning & Management
- (e) Packaging, Handling, Storage & Transportation
- (f) Technical Data
- (g) Support Equipment
- (h) Training & Training Support
- (i) Manpower & Personnel
- (j) Facilities & Infrastructure
- (k) Computer Resources

(l) Product Support Management

The product support elements are involved in the life-cycle management planning and acquisition strategy activities related to a system's modifications and upgrades, for both hardware and software items.

Depot-level Maintenance & Repair and Core Logistics Capabilities

Depot-level maintenance and repair (DLM&R) is defined in 10 U.S.C. 2460 as follows:

- “(a) In General.-In this chapter, the term "depot-level maintenance and repair" means (except as provided in subsection (b)) material maintenance or repair requiring the overhaul, upgrading, or rebuilding of parts, assemblies, or subassemblies, and the testing and reclamation of equipment as necessary, regardless of the source of funds for the maintenance or repair or the location at which the maintenance or repair is performed. The term includes (1) all aspects of software maintenance classified by the Department of Defense as of July 1, 1995, as depot-level maintenance and repair, and (2) interim contractor support or contractor logistics support (or any similar contractor support), to the extent that such support is for the performance of services described in the preceding sentence.
- (b) Exceptions.-(1) The term does not include the procurement of major modifications or upgrades of weapon systems that are designed to improve program performance or the nuclear refueling or defueling of an aircraft carrier and any concurrent complex overhaul. A major upgrade program covered by this exception could continue to be performed by private or public sector activities.
- (2) The term also does not include the procurement of parts for safety modifications. However, the term does include the installation of parts for that purpose.”

Unless a waiver is provided by the Secretary of Defense, not more than 50% of the funds made available in a fiscal year to a military department or a Defense Agency for DLM&R workload may be used to contract for the performance by non-Federal Government personnel of such workload for the military department or the Defense Agency.¹ This requirement is generally referred to as the “50/50 rule.”

The DoD is also required to establish and maintain a “core logistics capability” that is “Government-owned and Government-operated” (by the DoD) “to ensure a ready and controlled source of technical competence and resources necessary to ensure effective and timely response to a mobilization, national defense contingency situations, and other emergency requirements.”² These requirements are generally referred to as “Core.” While Core workload performed organically at public depots contributes to compliance with the 50-50 rule, DLM&R activities also include “non-Core” workload.

¹ See 10 U.S.C. 2466.

² See 10 U.S.C. 2464.

Linkage between the Life-Cycle Sustainment Plan (LCSP) (Product Support), the Intellectual Property (IP) Strategy, and the Acquisition Strategy

Data needed to plan, program, implement and oversee the product support (12 IPSEs) for a given weapon system includes form, fit, function, interface, operation, maintenance, installation, training and detailed manufacturing and/or process data with various levels of rights/licenses, to include: unlimited, Government Purpose Rights (GPR), negotiated, and limited/restricted based on the source of funding determination.

Since data requirements are generated from each of the 12 IPSEs, it is imperative that these data requirements (as well as those of systems engineering, test and evaluation, etc.), Government's data usage needs and the associated level of rights/licenses be identified in the IP Strategy in order to execute an approved Acquisition Strategy.

Limited Rights, When the System Development is Privately Funded, Does Not Impede Organic DLM&R

The Government generally obtains “limited rights” in technical data pertaining to items, components or processes developed exclusively at private expense, unless: (1) the parties negotiate otherwise, or (2) the data is of the type of data that the Government obtains unlimited rights in, regardless of the source of development funding (e.g., form, fit and function (FFF) data and data necessary for operation, maintenance, installation or training (OMIT)). Limited rights enables the Government to *“use, modify, reproduce, release, perform, display, or disclose technical data, in whole or in part, within the Government.”* Importantly, the Government may also release or disclose limited rights data to “covered Government support contractors” in performance of covered Government support contracts, for *“use, modification, reproduction, performance, display, or release or disclosure to a person authorized to receive limited rights technical data.”* Limited rights does not preclude the ability of the Government to perform organic³ DLM&R workload. However, the definition of limited rights prohibits the Government from using limited rights data for “manufacture.”

The manufacture of parts is not a routine DLM&R task, and the statutory definition of DLM&R does not expressly include the “manufacture” of spare/repair parts. However, Government panelists discussed the potential need for public depots to “manufacture” parts on an exception basis, such as in the case of diminishing manufacturing sources & material shortages (DMSMS) or emergency repair and overhaul of an end item (as opposed to routine, planned DLM&R), where there is an emergent supply and inventory issue that has or will imminently impact readiness. In these situations, public depots may identify a readiness-based need to manufacture a limited percentage of parts until: (1) the Government can procure the parts necessary to adequately fulfil inventory needs or (2) the Government otherwise performs a long-term workaround solution to the emergent DMSMS issue, such as reverse engineering. DoD guidance on DMSMS outlines proactive steps to anticipate and mitigate DMSMS issues.⁴ The DMSMS Guide says that “robust DMSMS management will secure data rights and bills of materials (BOMs) for items highly likely to face DMSMS issues.” The Guide also discusses the use of

³ “Organic” means employees of the Federal Government.

⁴ See SD-22 DoD Diminishing Manufacturing Sources & Material Shortages (DMSMS) Guidebook (January 2016).

reverse engineering as a solution to DMSMS issues. DMSMS issues should be proactively identified and mitigated, with IP needs addressed as part of the program IP Strategy. Thus, the need for public depots to manufacture parts in emergent DMSMS situations using limited rights data should be a rarity.

Depot-level maintenance requires industrial operations such as ‘building up’ a part whose wear limits require such action as opposed to manufacturing or ordering a completely new part. In such cases, the intent of the Government is not to manufacture a production run quantity of parts.

In accordance with the 50-50 rule, “*not more than 50 percent of the funds made available in a fiscal year to a military department or a Defense Agency for depot-level maintenance and repair workload may be used to contract for the performance by non-Federal Government personnel of such workload for the military department or the Defense Agency.*” Thus, “limited rights” does not inhibit the Government’s ability to comply with 50-50 rule requirements “*for the performance of depot-level maintenance and repair workload by employees of the Department of Defense.*”

Although “limited rights” does not impede organic DLM&R, it may impact the ability of the DoD to compete other types of acquisition activities, such as modifications, upgrades, contractor logistics support and the procurement of spare parts. These topics should be addressed as part of a program IP Strategy, in accordance with Department of Defense Instruction (DoDI) 5000.02.

Earlier Alignment between IP Strategies and Product Support Strategies is Needed

All Acquisition Category (ACAT) programs must have an acquisition strategy approved by a milestone decision authority.⁵ Each strategy must, where appropriate, include: (1) an intellectual property strategy in accordance with 10 U.S.C. 2320 and DoDI 5000.02 and (2) requirements related to all 12 IPSEs, which include but are not limited to 10 U.S.C. 2337 (Life Cycle Management), 10 U.S.C. 2464 (Core) and 10 U.S.C. 2466 (50/50 rule).⁶

The panel has noted in enclosure 1, table 2 of DoDI 5000.02 that core logistics determination/core logistics and sustaining workloads estimates are not required for Major Automated Information System Programs. The panel wonders whether or not this was an oversight. 10 U.S.C. 2460 defines depot-level maintenance, which includes depot-level maintenance of software, yet DoDI 5000.02 does not require ‘core’ estimates.

In addition to the acquisition strategy, a Major Defense Acquisition Program (MDAP) or subprogram may not receive Milestone A approval until the Milestone Decision Authority determines in writing, after consultation with the Joint Requirements Oversight Council, “*that planning for sustainment has been addressed and that a determination of applicability of core logistics capabilities requirements has been made.*”⁷ Further, a MDAP may not receive Milestone B approval until the Milestone Decision Authority determines in writing that “*life-cycle sustainment planning, including corrosion prevention and mitigation planning, has*

⁵ See 10 U.S.C. 2431a(a).

⁶ See 10 U.S.C. 2431a(c)(2)(F) and (J).

⁷ See 10 U.S.C. 2366a(b)(5) and DoDI 5000.02, dated 7 January 2015, Enclosure 1 Table 2, and Enclosure 6.

identified and evaluated relevant sustainment costs throughout development, production, operation, sustainment, and disposal of the program, and any alternatives, and that such costs are reasonable and have been accurately estimated.”⁸

10 U.S.C. 2320(e) also includes the following requirement, which is implemented in policy in Defense Federal Acquisition Regulation Supplement (DFARS) 207.106:

“The Secretary of Defense shall require program managers for major weapon systems and subsystems of major weapon systems to assess the long-term technical data needs of such systems and subsystems and establish corresponding acquisition strategies that provide for technical data rights needed to sustain such systems and subsystems over their life cycle. Such strategies may include the development of maintenance capabilities within the Department of Defense or competition for contracts for sustainment of such systems or subsystems. Assessments and corresponding acquisition strategies developed under this section with respect to a weapon system or subsystem shall—

- (1) be developed before issuance of a contract solicitation for the weapon system or subsystem;
- (2) address the merits of including a priced contract option for the future delivery of technical data that were not acquired upon initial contract award;
- (3) address the potential for changes in the sustainment plan over the life cycle of the weapon system or subsystem; and
- (4) apply to weapon systems and subsystems that are to be supported by performance-based logistics arrangements as well as to weapons systems and subsystems that are to be supported by other sustainment approaches.”

Enclosure 2 to DoDI 5000.02, Operation of the Defense Acquisition System, describes policies applicable to program managers. Program management must establish and maintain an IP Strategy as part of the Acquisition Strategy. The IP Strategy must be updated throughout the entire product life-cycle, initially as part of the Acquisition Strategy, and as part of the LCSP as part of the operations and support phase.⁹ However, only an IP Strategy summary is included as part of the Acquisition Strategy. The panel is concerned that if only a “summary” is required in the Acquisition Strategy, the IP Strategy will receive only summary-level treatment. A standalone IP Strategy may contribute to more complete IP analyses and expanded usage of appropriate rights/license arrangements, which might include Specifically Negotiated License Rights (SNLR) in situations where the Government desires greater rights than it would otherwise be entitled to under the regulations based on the funding determination.

Enclosure 6, paragraph 3.d.(2) to DoDI 5000.02, Life-Cycle Sustainment, requires Core Logistics Analysis to be included as an annex to the LCSP. By Milestone A, the DoD Component will document its determination of applicability of core depot-level maintenance and repair capability requirements in the LCSP in accordance with 10 U.S.C. 2366a. For Milestone B, the Program Manager will attach the program’s estimated requirements for maintenance, repair and associated logistics capabilities and workloads to the LCSP in accordance with 10 U.S.C. 2366b. The program managers must ensure that “a depot source of repair designation is made not later than 90 days after the Critical Design Review”. Before entering into a contract

⁸ See 10 U.S.C. 2366b(a)(3)(H).

⁹ See Enclosure 2 to DoDI 5000.02, page 76.

for low rate initial production, supportability analysis must include detailed requirements for core depot-level maintenance and repair capabilities, and associated sustaining workloads required to support such requirements. Program plans will include the use of Defense Logistics Agency (DLA)-operated storage and distribution facilities where collocated with the DoD Component's selection of organic depot maintenance.

In the absence of clear solicitation language outlining the product support strategy, contractors are required to make assumptions that they rely on in pricing their proposals, which includes how the offeror "values" its IP. The panel discussed that IP issues arise during performance of Engineering and Manufacturing Development (EMD) contracts when solicitations lack clarity or are silent on life-cycle sustainment plans and product support strategies. This contributes to disagreements between industry and the DoD regarding the scope and content of technical data deliverables and the associated rights and licenses. On the other end of the spectrum, some program offices have included solicitation language for EMD contracts directing offerors to assume "100% organic maintenance," presumably because source of repair designations have not been made or the customer is waiting until the supportability analyses and reliability testing have been completed to inform their decision.

The Government perspective is that within the Request for Proposal (RFP) exists a Statement of Work/Objective or Performance Work Statement which detail the actions required to execute the LCSP, its associated 12 IPSEs, and are supported by Contract Data Requirements Lists, which identify specific Data Item Descriptions that are supported by military and commercial specifications and standards. Examples of such requirements might include conducting product support analysis in accordance with SAE TA-STD-0017, logistics product data in accordance with SAE GEIA-STD-0007, the logistics product data handbook SAE GEIA-HB-007, preparation of digital technical information for interactive electronic technical manuals in accordance with MIL-STD-40051-1C, etc. Start of work meetings are utilized to discuss the requirements. Within the Program Manager's organization, the lead for the LCSP and all product support activities is the Product Support Manager who utilizes a Product Support Management Integrated Product Team (PSMIPT) to develop and execute the LCSP. The Original Equipment Manufacturer (OEM) is a member of the PSMIPT. Within the PSMIPT, one of the topics addressed is maintenance planning and management. Within that product support element, one of the tasks is planning and execution of depot-level maintenance to include core.

Greater emphasis on defining product support strategies and making depot source of repair designations, earlier in the acquisition life-cycle would yield better IP Strategies that may alleviate data delivery and data rights issues related to DLM&R that occur later in the acquisition life-cycle.

What if the Sustainment Strategy or Maintenance Concept Changes?

One issue which provided a consistent tension point is how the Department attempts to acquire technical data packages and sufficient license rights to perform sustainment when there is a change in the sustainment strategy. The change could be based on the program changing its maintenance philosophy (such as changing from planned program reliance on contractor logistical support to depot logistical support using competitor contractors). The change could

also come where a contractor OEM is no longer supporting the component, including where the contractor OEM no longer has a business interest in the component or is going out of businesses.

10 U.S.C. 2320(e)(3) already has a requirement that program managers account for such changes as part of their data and data/rights risk planning. However, program managers' ability to anticipate unforeseen sustainment requirements and future statutory, regulatory, or fiscal constraints in the out-years is challenging. At times it appears to industry that the inability of the program to anticipate such changes leads to a reflexive requirement to obtain all data with at least Government Purpose Rights and to order all data. At first glance, such a plan would work since the Government would have the data needed up front, and would also have the ability to use the data internally and maximize competitive acquisition and sustainment of the goods and services. Such requirements are considered by industry as being contrary to DoD policy in DFARS 227.7103-1 and 227.7203-1 in only acquiring the data and the data rights "necessary to satisfy agency needs." When this occurs, industry objects to the overreach of data acquisition and data rights which can by itself act as a limitation on competition for data only needed "just in case" of a programmatic change in strategy. Such upfront deliveries of data were reported by one government witness to cause logistical and storage problems due to the ordering of a "tsunami of data".

In addition, DFARS 227.7103-2 and 227.7203-2 charge a Data Manager or other requirements personnel with "identifying the Government's minimum needs" for technical data and software. However, both DFARS 227.7103-2 and 227.7203-2 require a Data Manager or other requirements personnel, to make very sophisticated analyses regarding future sustainment needs and philosophies.

Impacts to Readiness – Loss of Sustainment Support

The panel received briefings from DLA regarding impacts to readiness that have been attributed to data rights issues – whether due to the scope of the Government's license rights or a lack of access to technical data. Examples included DMSMS issues where sources of supply were limited or where OEMs exited a business or sold IP assets to third parties. Other examples related to sole source spare parts procurements where lead times had increased over time. DLA and a spare parts manufacturer also noted that, even if the Government has the technical data for an item, it does not always have the current version of the technical data which is needed for sustainment and maintenance.

Software Maintenance

Although DoD policy documents at one time defined "software maintenance," there is currently no DoD policy that defines software maintenance or software sustainment.

DLM&R, as defined, can be executed under 10 U.S.C. 2337 organically, commercially, through public-private partnership, or under performance-based arrangement. This is the same for a physical product as well as for a software product. If/when a specified maintenance task has been identified as a depot-level maintenance task and it is considered a core logistics capability, then it is an activity that is done by Government personnel in a Government operated facility.

However, there are fundamental differences between hardware and software maintenance. Unlike hardware-related DLM&R, where a logistician might repair or overhaul a widget to return it to service, software maintenance is more akin to a continuous software engineering process. The ISO/IEC/IEEE Systems and Software Engineering Vocabulary defines software engineering as “the application of a systematic, disciplined, quantifiable approach to the development, operation, **and maintenance** of software; that is, the application of engineering to software” (emphasis added).¹⁰ Software maintenance activities are similar to activities performed by software engineers during the initial software design and development (e.g., requirements definition and analysis, design, coding, testing, and the creation of documentation).

The applicable international standard for software maintenance, ISO/IEC/IEEE 14764, Software Engineering — Software Life Cycle Processes — Maintenance, identifies four categories of software maintenance, which are characterized as either providing **correction** or **enhancement**. This standard may be helpful in defining software maintenance, however this definition is broader than the statutory definition of DLM&R, which excludes “*the procurement of major modifications or upgrades of weapon systems that are designed to improve program performance.*”

A government work group defined software maintenance as including all actions that change the software baseline (adaptive, corrective, perfective, and preventative) as well as modification or upgrade that adds capability or functionality. This definition encompasses requirements development, architecture and design, coding, and integration and test activities. Industry’s view is that any DoD definition of software maintenance should exclude “*the procurement of major modifications or upgrades of weapon systems that are designed to improve program performance,*” consistent with the existing statutory definition of DLM&R.

Software Rights and Access to Software Design Information

Tension paper 13, Software versus Technical Data, discusses the differences between computer software and technical data. The DFARS defines “computer software” to include software design information such as source code, algorithms and other design details that would enable the software to be reproduced, recreated, or recompiled. Such software design information is analogous to detail manufacturing or process data (DMPD) pertaining to hardware and processes. While the DFARS definition of “computer software” includes software design information, it expressly excludes “computer software documentation” such as owner’s manuals, user’s manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software. Such computer software documentation is analogous to FFF data and OMIT data for hardware.

To perform all aspects of software maintenance, the DoD would need access to and delivery of both computer software and computer software documentation with some level of rights/license to enable the DoD to conduct software sustainment operations (inspect, test, check, repair, remove and replace, etc.). If the DoD does not have access to source code, or the rights necessary

¹⁰ *Guide to the Software Engineering Body of Knowledge (SWEBOK Guide), Version 3.0.*

to modify the software, then its ability to perform a full spectrum of software maintenance activities within the depots will be limited. The Government perspective is that a lack of access to source code may also impact the DoD's ability to satisfy strategic or contingency objectives.

Industry panelists noted that contractors and commercial software suppliers generally do not furnish source code and related software design information for commercial software or noncommercial software developed exclusively at private expense. In addition to maintaining IP protection, software owners are concerned about maintaining adequate configuration management of their code base to prevent unauthorized modifications or code "forks" that could introduce safety and security risks or maintenance challenges. In the case of aircraft, OEMs may have policies governing the release of any safety-critical system source code or related software design information related to commercial items, due to product integrity and safety concerns.

With the exception of open source software, commercial software end-user license agreements generally prohibit software modifications and reverse engineering. Unlike commercial software licenses, the DFARS definition of "restricted rights" permits both the Government and certain parties acting on the Government's behalf to modify software, with specified limitations. For example, the modified software must only be used with one computer at one time and may not be accessed by more than one terminal or central processing unit or time shared unless otherwise permitted by the applicable contract. In addition, the Government may only make the minimum number of copies of the computer software required for safekeeping (archive), backup, or modification purposes.

Source code access and IP licensing are important issues that should be considered as part of any business case analyses performed to determine the scope of organic software maintenance activities to be performed for a specific acquisition program. Such analyses should consider the extent to which the DoD system includes commercial software and noncommercial software developed exclusively at private expense.

Recommendation

We recommend no statutory changes to 10 U.S.C 2320 or 2321. The panel recommends regulatory changes identified below, as part of improved DFARS policy and guidance for SNLR agreements:

- 1) License language providing the Government with a right of first refusal to acquire rights or ownership to certain contractor technical data or computer software in the event the contractor decides to exit the business or no longer support a specified product or service (excluding mergers and acquisitions).
- 2) "Springing" or conditional licenses that are triggered by the occurrence of an event. For example, a right of first refusal may be triggered by a company's decision to exit the business and no longer support a specified product or service. Another example is a license that converts from limited rights to a broader SNLR license at a specific point in a program's life-cycle.
- 3) Direct licensing from OEMs to third parties for purposes of qualifying second sources, such as part of a "Spare Parts Acquisition Plan" (direct licensing as a possible licensing solution is already addressed in 10 U.S.C. 2320(a)(2)(I)(iii)).

- 4) The use of escrow arrangements, such as storing technical data or software, the release of which is subject to springing or conditional licenses.

Amend DoDI 5000.02 as follows:

- 1) Require program managers for all ACAT programs to develop standalone IP Strategy documents prior to Milestone B, to address all functional requirements with an eye toward life-cycle management. Each IP Strategy document should also specifically link to the applicable product support strategy, which must inform the identification of the Government's minimum needs for technical data and computer software.
- 2) Require program managers to describe the product support strategy as part of RFPs for the EMD Phase, such as by providing a summarized version of the current LCSP (e.g., delineating what is core and what is not). Require contractors to propose a product support strategy in response to RFPs for EMD contracts.

Establish DoD policy governing software maintenance and software sustainment that considers the following:

- Define software maintenance and sustainment, and the types of software modifications which may be performed as part of such activities;
- Identify the type of software to be covered by the policy. Source code access and IP licensing are important issues that should be considered as part of any 50/50 analyses.
- For software-intensive systems, require linkage between the IP strategy and a software configuration management plan, which will coordinate changes made by the Government, the OEM or third parties.
- A business case analysis should be performed as a prerequisite to performing software maintenance activities at public depots, and again before any changes to the sustainment strategy are made. The business case analyses should:
 - Address issues and topics that are unique to software maintenance/sustainment, including software lifecycle and obsolescence vs. the costs required to stand up an organic capability.
 - Consider whether organic sustainment is required by a strategic or contingency objective;
 - Consider whether capability is needed as a core logistics capability in accordance with 10 U.S.C. 2464;
 - Comply with DoDI 4151.20, depot maintenance core capabilities determination process;
 - Analyze whether Government performance of any such software maintenance activities is cost-effective (this is not the same as Office of Management and Budget Circular A-76). The analysis should include consideration of the capital investments, personnel, and IP needed to perform the activities;
 - Analyze the extent to which the DoD has sufficient access to, and IP rights in, software source code;
 - Consider the relevant skills and expertise of industry and the DoD depots;
 - Consider the extent to which the depots would be duplicating commercial industry capabilities.

13. Software versus Technical Data

Tension Point

The panel discussed the differences between “technical data” and “computer software” and whether technical data and software should be treated separately under applicable laws and regulations.

Issue

“Technical data” and “computer software” are inherently different, both from a functional and intellectual property perspective. Technical data delivered under Department of Defense (DoD) contracts generally describe technology (e.g., a drawing of a hardware item or the processes used to manufacture the hardware item¹), but computer programs (i.e., executable code), are technology. Further, source code, object code, and software design information such as algorithms, processes, flow charts and formulas that describe the design, organization, or structure of a computer program comprise the building blocks for the computer program.

Discussion

Reproducing copies of a computer program is akin to manufacturing additional quantities of a hardware item to which technical data pertain. However, computer software is unique in that a third party, whether skilled in the art or not, can reproduce additional copies of a computer program quickly and at a nominal cost, regardless of the time, private investment, know-how, testing and certification required to first design, develop and deploy a computer program. In comparison, manufacturing additional quantities of a hardware item using traditional manufacturing methods may be time- and cost-intensive, requiring access to: (1) the necessary technical data (e.g., drawings, manufacturing processes and test procedures) or the use of reverse-engineering methods; (2) know-how; (3) materiel; (4) any required tooling or test equipment and (5) testing and required certification.

The unique differences between computer software and technical data are reflected in the differences between the current Defense Federal Acquisition Regulation Supplement (DFARS) “limited rights²” and “restricted rights³” license grants. Whereas the Government receives a

¹ In the case of contracts for conceptual design or similar effort in which a contractor does not develop or deliver an item or process, a contractor may deliver technical data pertaining to design concepts, rather than an existing item or process.

² See DFARS 252.227-7013 (FEB 2014), paragraph (a)(14)

³ See DFARS 252.227-7014 (FEB 2014), paragraph (a)(15)

broad license to use, reproduce and disclose limited rights data internally within the Government, it receives a narrow license to use and reproduce restricted rights software –and may install restricted rights software on only one computer at a time and make copies only as required for archival, back-up or modification purposes.

Evolution of the Definitions

Enclosure 1 provides the statutory definition of “technical data” that has remained unchanged since 1984, the October 1988 DFARS definitions of “technical data,” “computer software” and “computer software documentation,” the current DFARS definitions (based on the 1995 rewrite), and the proposed changes to the definitions as set forth in the proposed 2010 DFARS part 227 rewrite. One of the key differences between the current DFARS definitions (based on the 1995 rewrite) and both the October 1988 and proposed 2010 definitions is the treatment of software design information such as algorithms, processes, flow charts, formulas and related information that describe the design, organization, or structure of a computer program.

In the early 1970s, the Enclosure 1 Armed Services Procurement Regulation (ASPR) data rights clause at 7-104.9 was modified so as to apply to both rights in technical data and rights in computer software. Previously, the ASPR data rights clauses addressed only rights in technical data. This approach continued until the 1995 DFARS rewrite, when the DoD established separate policies and contract clauses for technical data and computer software.

In the years leading up to the 1995 DFARS rewrite, three separate advisory panels provided recommendations related to technical data and software rights policy. The Blue Ribbon Commission on Defense Management (the “Packard Commission”), established via Executive Order 12526, recommended separate treatment of computer software in its 1986 final report.⁴

Appendix I to the report outlined specific recommendations, to include: (1) separate data rights clauses for technical data and software (to include the “associated documentation”) and (2) similar treatment of computer programs and the “associated documentation.”

Thereafter, the Acquisition Law Advisory Panel, established via Section 800 of the National Defense Authorization Act (NDAA) for fiscal year (FY) 1991 (the “Section 800 Panel”), recommended changes to the statutory definition of technical data.⁵ In its January 1993 report, the Section 800 Panel stated:

⁴ A Quest for Excellence: Final Report to the President by the President's Blue Ribbon Commission on Defense Management (June 1986), page 65, accessible at: <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA170887>

⁵ Streamlining Defense Acquisition Laws: Report of the Acquisition Law Advisory Panel to the United States Congress (January 1993), Chapter 5 Intellectual Property, page 5-24, accessible at: <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA262699>

“The current statutory definition of the term "technical data" was derived from the procurement regulations in 1984 when the statute was enacted. It excluded computer software **but included computer software documentation based on the current thinking in the Department. Since that time, almost all persons that have addressed the technical data and computer software policies have agreed that this is not a useful breakdown of intellectual property as it regards computer software.** The current thinking, as reflected in the Advance Notice of Proposed Rulemaking in October 1990, is that technical data should include computer data bases and manuals and other publications supporting computer programs **but that all elements of the computer programs themselves should be excluded from the definition of technical data.** The Panel agrees with this view and has recommended that the definition of "technical data" be revised to permit the new policy to be written on this basis” (emphasis added).

At the time, DFARS 252.227-7013, Rights in Technical Data and Computer Software (OCT 1988) defined “computer software documentation” to include source code and software design information such as algorithms. Like the Packard Commission, which recommended similar treatment of “computer software” and the “associated documentation,” the Section 800 Panel recommended that “all elements of the computer programs themselves should be excluded from the definition of ‘technical data.’” In its recommended changes to the statutory definition of “technical data,” the Section 800 Panel distinguished user documentation such as user’s manuals and installation instructions from source code, algorithms and other software design information that pertain to the internals of computer software.⁶

6.10.2.6. Proposed Statute

(8) the term "technical data" means recorded information of a scientific or technical nature. It does not include computer programs but does include manuals, instructional materials and technical data formatted as a computer data base, recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer software documentation) relating to supplies procured by an agency. Such term does not include computer software or financial, administrative, cost or pricing or management data or other information incidental to contract administration;

* * *

The following year, the Section 807 Government-Industry Technical Data Advisory Committee (the “Section 807 Committee”), formed in response to Section 807 of the NDAA for FY 1992 and 1993 (P. Law 102-190), also recommended separating “computer software” and “computer software documentation” from the technical data regulations, including further distinction between commercial and noncommercial computer software. The Committee noted that the

⁶ *Id.* at Chapter 6 Standards of Conduct, page 6-164.

separation “would provide greater flexibility to deal with evolving practices or statutory change relating to computer software with unintended impact on the technical data aspects of DoD’s regulations.”⁷ In its proposed changes to the definitions of “technical data,” “computer software” and “computer software documentation,” the Section 807 Committee addressed the concerns raised by the two prior advisory panels in recommending that “computer software” be broadly defined so as to include computer programs, source code and the associated software design information such as algorithms. In turn, the definition of “computer software documentation” was defined narrowly so as to include user’s manuals and other instructional materials while excluding software design information. The Section 807 Committee’s proposed definitions were subsequently adopted in the 1995 DFARS rewrite, which created separate clauses for rights in noncommercial technical data (DFARS 252.227-7013, the “-7013 clause”) and noncommercial computer software (DFARS 252.227-7014, the “-7014 clause”). The definitions recommended by the Section 807 Committee remain in the current DFARS today:

- (3) "Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation.
- (4) "Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

The Proposed DFARS Part 227 Rewrite

In the 2010 DFARS part 227 rewrite, the DoD proposed to combine the -7013 and -7014 clauses into one clause in order to streamline DFARS part 227 and the associated data rights clauses.

As part of the changes, the DoD proposed to revise the definitions of “computer software” and “computer software documentation” to reclassify computer software design documentation, such as design details, algorithms, processes, flow charts, formulas, and related information that describe the design, organization, or structure of computer software, as “computer software documentation” (a type of technical data) rather than “computer software.” The DoD proposed to reclassify these aspects of “computer software” as “technical data” because “these types of

⁷ Government-Industry Technical Data Advisory Committee Report to the Secretary of Defense (April 1994), Section II.F, page 2.

recorded information are more legitimately characterized as ‘technical data that pertains to an item’ (in this case, the item being computer software).’”

Industry’s concerns with the proposed treatment of software design information are as follows:

- 1) The fundamental design building blocks for a computer software program would be separated from the program itself, resulting in a situation where the Government would obtain broader rights in the software design information pertaining to software developed exclusively at private expense pursuant to a limited rights license, as opposed to a more narrow restricted rights license, even though industry is often more concerned about protecting software design information than executable code. Instead, industry’s view is that the Government’s rights in such software design information and the associated executable code should be consistent; the Government should not obtain broader rights to use software design information. This is consistent with the recommendations provided by the prior panels/committees that have explored these issues.
- 2) Hardware-oriented terms like “form, fit and function (FFF) data,” “data necessary for operation, maintenance, installation and training” (OMIT data), and the MOSA concepts of “major system interfaces” or other general interfaces could be applied to software design information.
- 3) There is uncertainty with regard to how the definition of “developed” would be defined and applied to software design information. Certain software algorithms and source code, such as that which pertain to flight controls, can be extraordinarily complicated and take many hours to develop. Under the current regulations, an algorithm may be “tested or analyzed to the extent sufficient to demonstrate to reasonable persons skilled in the art that the software can reasonably be expected to perform its intended purpose.” Under the proposed rewrite, the Government’s rights in the algorithm would be determined by the “item” to which the algorithm pertains. If the deliverable “item” is an executable computer program, then the Government’s rights in the algorithm could be determined by the source of funding used to merely compile the underlying source code into the deliverable executable computer program that is ultimately delivered to the Government. This result would disregard the substantial effort that went into designing and developing the software in favor of the trivial effort required to simply convert (with an automated tool) the computer software design and process steps into an executable computer program.
- 4) There will be confusion in practice, which could put industry data rights at risk, since “computer software documentation” is currently defined in the DFARS as user’s manuals and installation instructions to which the Government obtains unlimited rights. In accordance with the rewrite, the term would be redefined to include software design information, which may be deliverable with limited rights.

The Scope of the “Restricted Rights” License Grant May Not Meet the Government’s Operational Needs

The panel discussed practical challenges associated with restricting the installation of deliverable noncommercial restricted rights software on only one computer at a time. This restriction is particularly problematic for tactical software that must be installed on the entire family of the platform for which the software is intended, as well as in systems integration laboratories.

The Panel discussed the need to expand the scope of “restricted rights” to enable the Government to make a reasonable number of copies of noncommercial computer programs delivered with restricted rights to meet the Government’s programmatic needs, and when deployed, operational needs. The panel also discussed the need for the Government and industry to further analyze the Government’s needs of making additional copies of other elements of computer software, such as the related computer software design information, during the rulemaking process. This activity could involve reviewing software-related DIDs and Contract Data Requirements Lists to make specific recommendations.

Recommendation

The Panel recommends no statutory changes to 10 U.S.C 2320 or 2321.

The Panel recommends the following regulatory changes:

- 1) The treatment of computer software versus technical data be addressed in regulatory implementation with active industry participation, considering the factors discussed herein.
- 2) Combine the treatment of noncommercial computer software and noncommercial technical data into one DFARS clause that accounts for both the similarities and differences between computer software and technical data. For example, OMIT and FFF data could be defined so as to expressly include computer software documentation such as user’s manuals and installation instructions. This approach would provide continuing flexibility for addressing emerging and evolving issues that are unique to computer software and technical data, while at the same time streamlining the regulations. Examples include: (1) open source software, including any DoD initiatives to develop software in an open source environment and (2) the evolution of software development using model-based engineering approaches.
- 3) Broadening the “restricted rights” definition to enable the Government (but not parties acting on the Government’s behalf) to make a reasonable number of copies of noncommercial computer programs.

- 4) The implementing regulations and policy guidance should also address the Government's programmatic needs or operational needs, to copy other elements of noncommercial computer software.

Enclosure 1: Definitions

Term	10 U.S.C. 2302	DFARS 252.227-7013 RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE (OCT 1988)	DFARS 252.227-7013 RIGHTS IN TECHNICAL DATA— NONCOMMERCIAL ITEMS (FEB 2014)	Proposed 2010 DFARS Part 227 Rewrite
Technical Data	“Recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer software documentation) relating to supplies procured by an agency. Such term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration” (emphasis added).	“Recorded information, regardless of the form or method of the recording of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information” (emphasis added).	“Recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information” (emphasis added).	“Recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). The term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. Recorded information of a scientific or technical nature that is included in computer databases is also technical data” (emphasis added).
Computer Software	N/A	“Computer programs and computer data bases.”	“Computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation” (emphasis added).	“Computer programs; and source code, source code listings, and similar human-readable, recorded information that can be compiled to generate a computer program. The term does not include computer database or computer software documentation.”

Computer Software Documentation	N/A	<p>“Technical data, including computer listings and printouts, in human-readable form which (i) documents the design or details of computer software, (ii) explains the capabilities of the software, or (iii) provides operating instructions for using the software to obtain desired results from a computer” (emphasis added).</p>	<p>“Owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.”</p>	<p>“Technical data relating to computer software.</p> <p>(i) The term includes—</p> <p>(A) Computer software design documentation, such as design details, algorithms, processes, flow charts, formulas, and related information that describe the design, organization, or structure of computer software; and</p> <p>(B) Computer software user's documentation, such as user's or owner's manuals, installation instructions, operating instructions, and similar information that explains the capabilities of the computer software or provides instructions for using or maintaining the computer software.</p> <p>(ii) The term does not include computer software” (emphasis added).</p>
---------------------------------	-----	---	--	---

14. Development versus Adaptation (Majority Position)

Tension Point

In a data rights construct that is based largely on development funding, a tension arises whenever DoD funding is used to modify a privately funded or commercial technology, and it is not clear whether the modifications constitute development.

Issue

Regarding technical data, the long-standing framework at 10 USC 2320(a)(2) allocates relative rights of the Government and a contractor depending largely on whether the item or process to which the data pertain was developed by the contractor or subcontractor exclusively with Federal funds,¹ exclusively at private expense,² or with mixed funding.³ The scheme also recognizes a series of specific circumstances for which the baseline allocation of rights is altered.⁴ In addition to the allocation of rights, the source of development funding is also relevant for determining the availability of deferred ordering procedures, pursuant to the 2012 NDAA, as amended by the 2017 NDAA.⁵

In many industries relevant to the DoD's mission, it would be extremely rare to be able to apply or integrate any new technology -- no matter how mature -- to a particular platform or application without some form of modification (to either the underlying platform or the technology being integrated). In some (e.g., aerospace), it can be very expensive to implement and document even the most straightforward modifications. As opposed to the commercial aerospace (or shipbuilding or ground vehicle) marketplace, where technology providers and their customers generally rely on case-by-case negotiations to allocate the rights in any way that makes sense for a particular transaction, in the defense sector the parties often rely on standard or "default" rights established by the foregoing statutory/regulatory scheme as determinative. This foundational role of development funding is also reinforced by the DFARS procedures for asserting restrictions on deliverables, and the specialized statutorily-based procedures governing challenge and validation of such asserted restrictions.⁶

In addition, the DFARS implementation of this development-funding scheme in the context of commercial items has resulted in a process in which mixed development funding for the commercial item may appear to result in applying the noncommercial rules and procedures to commercial items. More specifically, when any portion of a commercial item has been

¹ Subparagraph (A)

² Subparagraph (B)

³ Subparagraph (E)

⁴ Subparagraphs (C), (D), (F), and (G)

⁵ Section 815(a)(2)(C)

⁶ See 10 U.S.C. § 2321 and DFARS 227.7103-10, -11, and -13 for tech data; and extended to computer software at 227.7203-10, -11, and -13 for computer software.

developed in any part at Government expense, the noncommercial tech data clause is prescribed to govern those portions, while the commercial clause remains applicable to the remainder of the commercial item that was developed exclusively at private expense.⁷ This may also lead to potential confusion in distinguishing “development” from “minor modifications” or “modifications of a type customarily [provided or] available in the commercial marketplace.”⁸

Therefore, what constitutes “developed” is important to determining rights in technical data (or computer software, pursuant to companion clauses⁹ in the DFARS) pertaining to both non-commercial and commercial items. A tension necessarily arises whenever a contractor uses (sometimes considerable) DoD funding to make modifications, and it is not clear whether the modifications constitute a “development.” Further, uncertainty as to whether the -7013 clause will apply to any given modification can disincentivize technology owners from using DoD funds to modify a privately funded or commercial technology to a DoD application if there is any chance that the modification will be viewed as development. Thus, the uncertainty can discourage the private sector from providing DoD access to innovative products, technologies, and processes developed for commercial use.

The term “developed” is defined in DFARS 252.227-7013(a)(7) as meaning that an item, component, or process exists and is workable.¹⁰ Thus, the item or component must have been constructed or the process practiced. Workability is generally established when the item, component, or process has been analyzed or tested sufficiently to demonstrate to reasonable people skilled in the applicable art that there is a high probability that it will operate as intended. Whether, how much, and what type of analysis or testing is required to establish workability depends on the nature of the item, component, or process, and the state of the art. To be considered “developed,” the item, component, or process need not be at the stage where it could be offered for sale or sold on the commercial market, nor must the item, component, or process be actually reduced to practice within the meaning of Title 35 of the United States Code.

To provide certainty, and therefore promote DoD access to innovative technologies, this framework needs to be clarified regarding best practices and consistent approaches for analyzing: (1) the extent to which items, components, processes or computer software have been

⁷ DFARS 227.7102-4(b). Note this approach of prescribing the noncommercial clause for portions of the technology is not implemented for commercial computer software that was developed in any part at Government expense.

⁸ See definitions of “commercial item” at FAR 2.101, and “commercial computer software” at DFARS 252.227-7014(a)(1) (compare CCS definition at FAR 2.101, which DoD has indicated desire to adopt (see DFARS Case 2010-D001)). These types of modifications are relevant in determining whether a technology is commercial or noncommercial, but do not directly affect the default rights category (i.e., unless the modification also qualifies as development). The term “provided” is used in DFARS definition of “minor modification”; the term “available” is used in the FAR definition of “commercial item”

⁹ DFARS 252.227-7014

¹⁰ Note the term is defined slightly differently in the context of noncommercial computer software at 252.227-7014(a)(7), although the definitions retain the two-pronged test of (i) exists and (ii) is workable.

“developed” for data rights purposes and (2) the type and nature of modifications to be performed under prospective contracts.

Recommendation

The Panel supports the statutory revisions proposed in (*Tension Paper 19, mandatory flow-down (commercial subs and suppliers)*) regarding the non-applicability of certain elements of the statutory requirements to technical data related to adding flexibility for the Government and contractors to negotiate the applicability of the validation scheme to other commercial items and the streamlining and clarification of the presumptions of development at private expense, as those revisions will also address some of the issues raised in this paper regarding uncertainty resulting from the application of the development funding criteria, including through a validation procedure, may affect the parties rights.

(Same change as Tension Paper 19) Amend 10 USC 2321 as follows:

(a) This section applies to any contract for supplies or services (except for commercially available off-the-shelf items, as defined in section 104 of Title 41) entered into by the Department of Defense that includes provisions for the delivery of technical data. In the case of all other commercial items, this section shall apply except to the extent specified in the contract in accordance with criteria specified by the Secretary to balance the respective interests of the United States and the contractor or subcontractor.

The Panel recommends the following regulatory changes:

The commercial technical data clause, 252.227-7015, should be revised to include an Alternate version that allocates rights between the parties in cases when some portion of the commercial item has been developed at least in part with Government funds, to avoid the requirement to apply the noncommercial clause to a commercial item (which may appear to be based on a determination that the item is not a commercial item). The Alternate version of the clause should be structured to allow the parties to specify their mutual agreement (if any) regarding how the alternate Government-funding portions of the clause will be applied or “map” to the various

items, components, or data deliverables.¹¹ An analogous alternate clause structure could also be used to map the applicability of the validation procedures.

The DFARS, PGI, and other guidance should also clarify the allocation of rights between the Government and contractor for commercial computer software (CCS) that has been developed in some part with Government funding. The guidance should provide a preference for negotiation of such rights in the CCS license or an addendum thereto. (This approach is consistent with current DFARS policy, since there is no DFARS clause prescribed for CCS¹²).

In addition, the Panel recommends the following:

Issue guidance encouraging the use of negotiated licenses to allocate IP rights between the parties in the case of a contract for the modification of a commercial technology to a Government application.

Issue guidance to, wherever appropriate, capture in the statement of work the parties' understanding, expectations, and agreement regarding what modifications will be made (cross-linked to anticipated costs), which modifications would constitute development for source-of-funding data rights allocation purposes, and perhaps boundary conditions or criteria (e.g., percent change in cost, cascading impacts on other systems/components, etc.) by which the parties' agreement would need to be revisited. Such documentation will be useful in helping the parties ascertain whether future changes in circumstances warrant revisiting the decisions that were made at contract formation.

Issue guidance regarding the appropriate use of other established technology development schemes (e.g., technology readiness levels , manufacturing readiness level; the research,

¹¹ For example, the alternative version may allow the parties to record their agreement that the Government-funding elements added by the clause will apply only to certain items, or that those elements will not apply to certain other items, or both. Similarly, this mapping could be accomplished by including both the Basic and alternative versions of the commercial clause, and allowing the parties to specify which commercial items each clause applies to, or does not apply to.

¹² Note: In the DFARS FR notice for the 1995 DFARS rewrite final rule (60 FR 33464, 28 Jun 1995), the DARC addressed public comments expressing concern USG losing rights in USG-funded software subsequently qualifying as CCS: “8. Computer Software. Thirteen comments addressed computer software. Three commentors suggest the definition of “commercial computer software” is too broad. One also suggests that the definition’s broad scope will make it difficult to understand and interpret and contractors will be able to restrict the [*33467] Government’s rights in software developed exclusively at Government expense by satisfying one of the criteria that define commercial computer software. Those suggestions are not adopted. The definition of commercial computer software has been modified to reflect requirements in the Federal Acquisition Streamlining Act of 1994. The Government will not lose rights obtained in software developed at government expense if that software subsequently qualifies as commercial computer software. That situation is covered by 252.227-7014(b)(5) [(the “prior Government rights” license category)] and (c) [(“rights in derivative [CS] or [CSD])].”

development, test, and evaluation budget activity categories) as considerations for assessing whether an item to be developed or modified has been “developed” for data rights purposes. Such guidance should include “boundary” examples of cases in which modifications do and do not reach the level of development. Similarly, the guidance should reinforce appropriate distinctions between these various schemes and criteria, to help mitigate against the *inappropriate* application of one scheme’s criteria as being determinative in a different scheme. For example, the fact that a particular system may not have achieved a certain TRL overall does not mean that none of its subsystems or components could very well have already met the criteria to be “developed.”

Issue guidance to reinforce and clarify that the mere fact that Government funding has been used to modify a commercial item or a noncommercial item that had previously been developed exclusively at private expense is not sufficient to serve as the sole basis for supporting a successful Government challenge to asserted restrictions on the technical data pertaining to the underlying item. In these circumstances, the Government funded modification must meet the criteria to qualify as “development” to affect the allocation of default license rights based on the source of development funding.

Minority Report

14 Development versus Adaptation (Minority Position)

Authors: Elliot Branch, Joseph Gordon, Roger Hamerlinck, Theodora Hancock, Charles Harris

Proposal

Seven of the twelve panel members, i.e., six industry panel members and one Government panel member (hereinafter “Majority members”) suggested a legislative proposal to eliminate mandatory flow-down requirements for commercial items in Paper 19. The remaining five panel members, all from the Government, (hereinafter “Minority members”) provided a Minority Position regarding mandatory flow-down of clauses for commercial items in a Minority Position regarding Paper 19.

The Majority members now propose *again* certain of the *identical statutory changes* from the mandatory flow-down paper to solve a completely different problem, i.e., an engineering problem of identifying whether modifications to an existing item constitutes Development or mere Adaptation.

The Majority Position also presents a narrowly tailored regulatory change to the DFARS clause at 252.227-7015 to address the problem of Development versus adaptation.

The Majority Position further includes additional regulatory recommendations that, if adopted, would present various approaches to solving the Development versus Adaptation dilemma.

Minority Proposed Compromise: The Minority members agree that unnecessary administrative burdens can and should be addressed during the rulemaking process. The Minority members worked cooperatively with the Majority members to create some of the proposed regulatory changes.

The Minority members state here, as in paper 19a, that there is no need for statutory changes, when rulemaking will suffice. Additionally, any rulemaking should be narrowly tailored to address the specific problem at issue.

Discussion

The Minority members note that research and development (R&D) contracting involves significant risk for the Government. First, the Government annually provides billions of dollars of R&D funding with no guarantee that the contractor efforts will be successful. Next, the Government provides a design specification and relies on the contractor, in the contractor’s own discretion, to employ a technical approach. Finally, the Government must be prepared, for the contractor, after accepting Government funding to develop a new technology, to argue that the

billions of dollars in Government funding resulted in all IP rights belonging to the contractor and none to the Government.

The source of funding test for development has persisted for decades as there is simply no better test for allocation of IP rights in Government contracts. The Majority members seek to further remove any risk from the contractor and to transfer that risk to the Government with this proposal. It is important to note that the contractor, not the Government, controls the technical approach and the decision of whether or not to use Government or contractor funding during a Government contractor. This proposal, if adopted, would allow a contractor, through negotiation, to transfer all R&D risk to the Government, accept billions of dollars in Government funding, and retain all IP rights without providing any IP rights to the Government. This proposal would also violate the section 813 statutory direction to ensure “that the Department of Defense does not pay more than once for the same work.”

This proposal does not meet the needs of the DoD because it does not serve the interests of the warfighter. The Majority Report recommendations do not serve the direction of Congress.

CASE-BY-CASE APPLICATION OF DATA RIGHTS VALIDATION STATUTE REGARDING MODIFIED COMMERCIAL ITEMS

The Majority members propose a final sentence to 10 USC 2321(a) to allow the applicability of the validation statute, which protects the interests of the warfighter and the taxpayer, to be altered or removed on a case-by-case basis. The Panel members acknowledge that a non-COTS commercial item initially developed at Government expense could be subsequently sold or offered for sale to the Government as a commercial item. In other words, an item fully funded by the Government might later be re-characterized as a commercial item and the Government would lose the benefit of its funding with respect to intellectual property rights unless the Government meticulously maintains the relevant contract documents in order to challenge the re-characterization. Further, industry supports this rebuttable presumption, even though it may result in Government funding being subsequently treated as industry funding. The Panel members want to incentivize industry to make investments in new technologies. It is not at all clear that adding more complexity to these already complex rules would spur industry investment. To the contrary, industry may be incentivized to utilize more clever lawyering or accounting, e.g., to use all Government funding to develop dual-use technologies. At some point commercial sales of that fully-Government funded technology would trigger a re-characterization, so the Government would lose its rights in that fully-Government funded technology unless the Government somehow tracked the industry product and maintained the related-financial records. It is unclear how this lawyering or accounting-based windfall to industry is a fair and equitable resolution of the tension point regarding development versus adaptation of technology.

The Minority members prefer statutory changes that incentivize industry to provide technically superior products or more affordable products. The Minority members see no value in rewarding industry for creative lawyering or creative accounting. Statutory changes such as case-by-case application of commercial item status (re-characterization addressed above), case-by-case applicability of deferred ordering, or case-by-case applicability of the data rights validation

statute, reward creative lawyering or creative accounting, in our view, and do not bring better, more affordable capabilities to the warfighter. To the contrary, the Department of Defense may be vendor-locked and forced into a sole source position for decades, which is to the detriment of the taxpayer (due to lack of cost control) and to the detriment of the warfighter (due to lack to better or more affordable technology).

Recommendation:

We concur with the Majority members' proposed regulatory changes. We also concur with the Majority members duplicative recommendation from Paper 19a regarding a COTS exception to 10 USC 2321.

We urge the Secretary of Defense to **non-concur** on the statutory proposal regarding 10 USC 2321(a) for "all other commercial items", in his recommendations to the congressional defense committees for the following reasons:

- The proposal unduly increases DoD's risk regarding organic sustainment of its weapons systems and unduly decreases potential competition in future procurements
- The proposal unduly limits DoD implementation of MOSA
- It unduly limits small business participation in defense contracts
- It unduly increases vendor-lock which will exacerbate the excessive pricing that DoD has experienced and will continue to experience for the foreseeable future.
- It does not serve the needs of the warfighter in the dynamic realm in which DoD operates.
- It does not serve the interest of the American taxpayer.

15. Operation, Maintenance, Installation, and Training (OMIT) Data versus Detailed Manufacturing or Process Data (DMPD), including such data pertaining to a major system component

Tension Point

Current statute and policy requires unlimited rights for data necessary for the purposes of OMIT (other than DMPD) and allows restrictions to be placed on DMPD.

Issue

When does data needed to identify and perform maintenance become detailed manufacturing or process data?

Discussion

10 U.S.C. 2320 outlines the requirement for regulations to apportion basic rights for data afforded to the Government based on funding determinations (private funding, mixed funding, or government funding). 10 U.S.C. 2320(a)(2)(C)(iii) states “Subparagraph (B) does not apply to technical data that is necessary for operation, maintenance, installation, or training (other than detailed manufacturing or process data, including such data pertaining to a major system component);...” 10 U.S.C. 2320(a)(2)(D)(i)(I)-(III) states “Notwithstanding subparagraph (B), the United States may release or disclose technical data to persons outside the Government, or permit the use of technical data by such persons, if such release, disclosure, or use is necessary for emergency repair and overhaul; 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; or is a release or disclosure of technical data (other than detailed manufacturing or process data) to, or use of such data, by a foreign government that is in the interest of the United States and is required for evaluation or information purposes.” 10 U.S.C. 2320 (a)(2)(D)(ii)-(iii) state “such release, disclosure, or use is made subject to a prohibition that the person to whom the data is released or disclosed may not further release, disclose, or use such data; and the contractor or subcontractor asserting the restriction is notified of such release, disclosure, or use.”

In its implementing clause for non-commercial items, the Defense Federal Acquisition Regulation Supplement (DFARS) 252.227-7013(a) defines DMPD as “technical data that describe the steps, sequences, and conditions of manufacturing, processing or assembly used by the manufacturer to produce an item or component or to perform a process.” A similar definition exists for commercial items in DFARS 227.22-7015.

The Secretary of Defense through the Under Secretary of Defense for Acquisition, Technology and Logistics has delegated to the Assistant Secretary of Defense for Logistics and Materiel Readiness (ASD (L&MR)) authority to prescribe policy and procedures for the conduct of logistics, maintenance, materiel readiness, and sustainment support.

The ASD(L&MR) implements statutes (10 U.S.C. 2337, Life-cycle Management and Product Support; 10 U.S.C. 2460, Definition of Depot-level Maintenance and Repair; 10 U.S.C. 2464, Core Logistics Capabilities; 10 U.S.C. 2466, Limitations on the Performance of Depot-level Maintenance of Materiel; 10 U.S.C. 2474, Centers of Industrial and Technical Excellence: Designation; Public-Private Partnerships; etc.) through the publication of policies (e.g., Department of Defense Directive 4151.18, Maintenance of Military Materiel; Department of Defense Instruction 4151.20, Depot Maintenance Core Capabilities Determination Process; etc.) and other guidance documents.

To comply with and execute these statutes, policies, and guidance documents published by the Department of Defense (DoD); Military Departments and defense agencies have a need for technical data, computer software documentation, computer software, and the associated rights and licenses, in support of the OMIT activities for military equipment and software across all echelons. DFARS 252.227-7017 (the data assertion list), paragraphs (b)-(d), require the contractor to identify the technical data, computer software documentation, and/or software that will be delivered with less than unlimited rights or where restrictions to use, release, or disclose the data is contemplated. These guidance documents are for the functional workers and do not connect OMIT activities to the DFARS technical data license concepts in DFARS 252.227-7013 and 252.227-7015. They also do not relate assertion lists which would provide notice to the functional workers of potential use restrictions when the technical data is delivered or whether these restrictions impact the Intellectual Property (IP) Strategy for sustainment of the program.

MIL-STD-31000A, Department of Defense Standard Practice for Technical Data Packages defines a Technical Data Package (TDP) as “a technical description of an item adequate for supporting an acquisition, production, engineering, and logistics support (e.g., Engineering Data for Provisioning, Training, and Technical Manuals). The description defines the required design configuration or performance requirements, and procedures required to ensure adequacy of item performance. It consists of applicable technical data such as models, drawings, associated lists, specifications, standards, performance requirements, quality assurance provisions, software documentation, and packaging details.” It also defines Supplementary Technical Data as “data related to or in support of a TDP, but not an inherent part of the TDP, which is provided as reference material or is explanatory in nature. For example, Supplementary Technical Data for a particular configuration item could include manufacturing instructions, simulations, work flow data, inspection equipment or procedures (which are not required as an inherent part of the TDP or TDP element), manufacturing machine code, design studies, analysis studies, test results,

safety data sheets, etc.” MIL-STD-31000A is for the functional worker and does not connect OMIT activities to the DFARS technical data license concepts in DFARS 252.227-7013 and 252.227-7015 (especially in regard to restrictions on detailed manufacturing or process data), or whether these restrictions impact the IP Strategy for sustainment of the program.

ASME Y14.24-2012, Types of Engineering Drawings, identifies 12 general types of engineering drawings. While this standard discusses manufacturing planning, none of the types of engineering drawings are identified as detailed manufacturing or process data. The Panel is also not aware of any guidance which would alert a functional worker as to which types of drawings are likely to contain DMPD (which has the potential for restrictions on use), and which are less likely to contain DMPD, and whether the potential use or release restrictions in DMPD impact the IP Strategy for sustainment of the program.

The Military Departments obtain data through the application of commercial and/or military specifications and standards, Data Item Descriptions (DIDs), and Contract Data Requirements Lists (CDRL) placed in contracts. Examples include, but are not limited to: DI-SESS-81716, Supplemental Provisioning Technical Documentation; DI SES-81758A, Logistics Product Data with GEIA-STD-0007; DI-PSSS-81872A, Level of Repair Analysis with SAE/TA-STD-0017; MIL-HDBK-1222F, Guide to the General Style and Format of U.S. Army Work Page Technical Manuals; MIL-STD-40051-1C, Preparation of Digital Technical Information for Interactive Electronic Technical Manuals or MIL-STD-50051-2, Preparation of Digital Technical Formation for Page-Based Technical Manuals (TMs); and MIL-PRF-32216A, Evaluation of Commercial-Off-The-Shelf Manuals and Preparation of Supplemental Data with DI-TMSS-80527C, Commercial-Off-The-Shelf Manuals and Associated Supplemental Data or DI-TMSS-80528, Supplemental Data for Commercial-Off-The-Shelf Manuals. Contractors rely on the DIDs to provide the level of data for these reports and manuals prepared under a contract, which allows for the possibility of use restrictions where DMPD is required by the content of the DID. The Panel is also not aware of any guidance which would alert a functional worker as to whether a particular DID is likely to contain DMPD, whether the potential use or release restrictions impact the IP Strategy for sustainment of the program, and if there is an impact, how to tailor the DID to meet the IP Strategy.

Joint Regulation Governing the Use and Application of Uniform Source, Maintenance, and Recoverability Codes (SMR) (Army Regulation 700-82, Secretary of the Navy Instruction 4410.23, and Air Force Manual 21-106): The SMR code provides maintenance activities with repair level responsibilities, support method (that is, procure, manufacture, etc.), and disposition instructions. This publication reflects the changes in terminology required by the performance specification, TechAmerica Government Electronics & Information Technology Association – Standard-0007. Source codes are assigned to support items to indicate the manner of acquiring support items for maintenance, repair, rework, or overhaul of end items and to identify items

requiring special handling. “M” source coded items are to be manufactured or fabricated at specified maintenance activities. They are normally consumable items or those requiring very limited repair. Typical M series coded items (eg. hose assemblies, tubing, name plates, decals, and wires), have minimal likelihood of replacement during the life cycle of the end item. All the publications, manufacturing data, and required shop equipment and skills must be available at the specified maintenance activity. Maintenance codes are assigned to indicate the level of maintenance and/or maintenance activity authorized to use, remove, replace, or repair support items. Recoverability codes are assigned to support items to indicate the disposition action on unserviceable items. The Panel is not aware of whether the recoverability codes are used in the creation of an IP Strategy for program sustainment, as well as whether the codes are used to ensure the correct data is being ordered based on the Depot’s assessment of repair levels for supported items.

The DoD considers the following to be representative of, but not all inclusive of, typical preventive and corrective maintenance tasks: inspection, testing, servicing, repair, rebuilding, reclamation, adjusting, alignment, calibration, removal, replacement, paint, overhaul, lubrication, preservation, assembly/disassembly, cleaning, radio interference suppression, towing, jacking, parking, mooring, covering, hoisting, sling loading, preparation for storage, preparation for shipment/transportation, arming, loading, unloading, installing/uninstalling peripheral devices, upgrade/patch, configure, debug, and diagnostics/prognostics.

In the fiscal year 2017 National Defense Authorization Act, 10 U.S.C. 2320 was amended to state that DMPD further includes data pertaining to a major system component. In essence, for an item/software that is privately funded, DMPD is the manufacturer’s “secret sauce” on how they manufacture a component. When DMPD is not delivered, this means certain Depot activities may not be possible since the content of the data may not meet Depot requirements (especially for D level maintenance). However, where DMPD is delivered for OMIT activities and is subject to Limited Rights or Commercial Rights, the data licenses under DFARS 252.227-7013 and 252.227-7015 restrict the use purely to Government personnel performing repairs organically.

The Panel received multiple comments and had multiple discussions on the relationship between data necessary for OMIT and DMPD. The Panel is unaware of a DoD document which aligns existing functional user documentation and routines (such as Depot instructions) with the legal definition of data necessary for OMIT, or how rights in the data affect Depot responsibilities for performing their duties.

The Panel recognizes this as an issue since Depots are required to perform such activities by 10 U.S.C. 2464 (“organic core capability”) and 2466 (“50-50 rule”). Since DMPD can be Limited Rights or Unlimited Rights depending on the levels of Government or contractor development,

the Panel notes that the potential for restrictions on DMPD and Limited Rights might represent a risk to the Depot to perform organic standup where local manufacturer of parts is required, and comply with the 50-50 rule if third party contractors are required, but not very often.

The Panel received numerous industry comments that consistently indicate a normal industry reaction is to reach an agreement with particular customers for performing detailed repair/manufacturing processes. These agreements take into account the component Original Equipment Manufacturer's (OEM) business expectations, and also account for quality/qualification issues. This is consistent with DFARS guidance in DFARS 227.7103-5(d)(2).

The Panel also discussed the use of reverse engineering, with industry comments confirming that reverse engineering is a normal industry reaction to a lack of data (subject to firewall protections and patent searching). The Panel is aware of Government activities which create data through reverse engineering for the purpose of manufacturing parts when there is a diminishing supply issue.

The Panel received specific comments from academia on the necessity of setting up second sourcing agreements. These comments are consistent with Panel discussions on the need to set up transition agreements, use escrow agreements, use public private partnerships, and create standard Specifically Negotiated Licenses tailored to Depot activities. These recommendations have been made in other sections. The industry members of the Panel are not aware of the Depots having any specific instructions or standard agreements which a program or contracting officer can utilize for these agreements, and note the standard in the industry is to have such templates to encourage solutions to meet customer unique requirements.

The Panel received Government comments that Depots are unable to compete their maintenance functions unless DMPD is made unlimited rights, and non-OEM industry comments concur since they want to compete with the OEM for Depot work. Some of these comments relate to Federal Aviation Administration processes in relation to continued airworthiness instructions, although OEMs have maintained such instructions generally lack DMPD and are therefore consistent with current DFARS definitions of OMIT data.

The Panel also received information from OEMs who indicate that they rely on restrictions on the DMPD as part of their business model, which is based on aftermarket support and services. They maintain that if DMPD is made Unlimited Rights like the rest of data necessary to perform OMIT, OEMs will not be able to make the business case to privately develop components and systems to sell to the Government. In such a case, they contend Government would need to fund the entire development of all systems or subsystems since they would refuse to bid on work which places privately funded and commercial systems or subsystems at risk. Industry members

have noted supply chain resistance and no-bids on subcontracts which specifically require delivery of data necessary for OMIT if provided with Unlimited Rights.

Recommendation

The Panel recommends no change to 10 U.S.C. 2320 or 10 U.S.C. 2321.

The Panel recommends a guide with definitions, key terms, and examples that distinguish DMPD which is entitled to restrictions where privately funded, as an exception to OMIT that qualifies for Unlimited Rights. The Guide could have a format similar to that provided in the Department of Defense Guidebook for Acquiring Commercial Items (February 24, 2017). The Panel recommends an update to DFARS 227.7103-5(d)(2) to address Depot requirements, and specifically the types of rights needed for Depot maintenance in the scope of 10 U.S.C. 2460 and alternatives in the instance when the contractor is unwilling to license specific maintenance activities. Adapt similar guidance to Depot requirements for non-commercial computer software at DFARS 227.7203-5, commercial technical data at DFARS 227.7102, and commercial computer software at DFARS 227.7202.

16. Rigid Intellectual Property (IP) Requirements versus Flexible Arrangements

Tension Point

The existing Defense Federal Acquisition Regulation Supplement (DFARS) data rights provides a default position which is appropriate for most transactions, but does not cover all situations where flexible arrangements might be more appropriate.

Issue

The Panel received information about the sufficiency of the existing data rights allocation, and generally concluded that even Limited Rights or Restricted Rights would be sufficient for most internal Governmental needs. Where the Government has specific needs which are not met by the Limited Rights and Restricted Rights licenses, both DFARS 252.227-7013 and 252.227-7014 provide authority to the contracting officer to change the rights allocation to meet the Government's needs. Industry has noted that such authority is bounded since the Government cannot accept licenses below a Limited Rights license, which provides a "royalty free, worldwide, nonexclusive, irrevocable license rights in technical data" within the Government.

Discussion

The Panel received industry comments that the default license rights for Unlimited Rights and Government Purpose Rights in DFARS 252.227-7013 and 252.227-7014 are unnecessarily broad. Further, industry commented that Government Purpose Rights is indistinguishable from Unlimited Rights for Department of Defense technologies (with the exception that Unlimited Rights would allow the data to be shared on the internet), which provides a strong disincentive to industry delivering data subject to these licenses. The Panel also received information from Government representatives that Limited Rights or Restricted Rights data license may not be sufficient for achieving particular agency missions, such as performing depot level repairs or upgrades to systems.

To the extent that the Government attempts to resolve these issues by changing the default license categories or rely on inchoate rights and deferred ordering mechanisms to mandate delivery of data which the contracting parties specifically removed from a contract, industry representatives commented that these policies will result in fewer deliveries or incomplete data sets which will still prevent agencies from meeting their needs. The Panel received information that increased demands for data deliveries and data rights can reduce competition for proposals with such demands.

In this situation, industry noted that Specifically Negotiated Licenses (SNLR) could serve the Government's interests by tailoring the rights to accommodate both parties' interests. Industry also commented that contracting officers are reluctant to negotiate SNLR more restrictive than Government Purpose Rights, even where such licenses would encourage industry to deliver more data and such licenses would meet the Government's minimum needs. The Panel received Government comments that SNLR are difficult to negotiate, and that there are too few Government personnel available with enough experience, who are qualified to negotiate SNLR. Industry representatives noted that the industry standard is to have example SNLR for specific situations, and suggested that the Government could benefit from a library of SNLRs for specific situations and additional training to contracting professionals, who could tailor the SNLR for specific situations.

The Panel also received an industry suggestion that templates for SNLR could include Specifically Negotiated Licenses with advanced waivers from Defense Procurement and Acquisition Policy to allow licensing below the normal Limited Rights and Restricted Rights licenses in DFARS 252.227-7013 and 252.227-7014. Such specialized licenses could also use specific clauses, such as Depot Repair specific clauses which allow DoD depots to acquire technical data packages with usage limited to the particular depot and which limits usage to only qualified personnel. Such a specialized clause is consistent with industry examples provided to the Panel of how industry licenses third party maintenance and repair entities while ensuring the safety and adequacy of the repairs.

The Panel also received information from Government agencies which use flexible arrangements, mainly Other Transactions (OTA) or Technology Investment Agreements (TIA), to access data and technologies where intellectual property concerns might otherwise provide a barrier to contracting under normal DFARS processes. Such flexible arrangements could allow Government agencies to negotiate below the normal Limited Rights licenses, including limiting the geographical or government distribution of the data provided under such licenses.

While OTAs or TIAs are generally limited to research and development work, industry representatives have suggested that depots and labs could similarly use their non-FAR based authorities to create similar flexible arrangements. Examples of such arrangements could be Commercial Services Agreements or Public Private Partnerships, both of which have an additional advantage in that the Government personnel could also receive knowhow and training as opposed to simply a copy of written technical data or computer software.

Recommendation

The Panel does not recommend any changes to 10 U.S.C. 2320 or 2321.

The Panel recommends that the following changes be made to the DFARS:

DFARS 227.7103-5, Government rights.

The standard, default license rights that a licensor grants to the Government are unlimited rights, government purpose rights, or limited rights. Those rights are defined in the clause at 252.227-7013, Rights in Technical Data—Noncommercial Items. In usualmany situations, the standards standard, default rights may not satisfy the Government's or the Contractor's needs or the Government may be willing to accept lesser rights in data in return for other consideration or to encourage competition. In those cases, contracting officer is encouraged to consider negotiating a special license may be negotiated to achieve a mutually agreeable solution. However, while these standard, default rights are starting points of such a negotiation, the licensor is not obligated to provide the Government greater rights and the contracting officer is not required to accept lesser rights than the rights provided in the standard grant of license. The situations under which a particular grant of license applies are enumerated in paragraphs (a) through (d) of this subsection.

**

(d) *Specifically negotiated license rights.* (1) Negotiate specific licenses when the parties agree to modify the standard license rights granted to the government or, when the government wants to obtain rights in data in which it does not have sufficient rights under the standard license rights, or when the government wishes to reduce its standard license rights in return for other consideration or to encourage competition. When negotiating to obtain, relinquish, or increase the Government's rights in technical data, the contracting officer shall, in consultation with agency Intellectual Property counsel, consider the acquisition using pre-approved specific licenses provided agency Intellectual Property counsel as a starting point for such negotiations, consider the impact of the on Intellectual Property strategy for the item, component, or process, including logistics support and other factors which may have relevance for a particular procurement. The Government may accept lesser rights when it has unlimited or government purpose rights in data but may not accept less than limited rights in such data except as authorized by agency Intellectual Property counsel. The negotiated license rights must stipulate what rights the Government has to release or disclose the data to other persons or to authorize others to use the data. Identify all negotiated rights in a license agreement made part of the contract.

DFARS 227.7203-5, Government rights.

The standard, default license rights in computer software that a licensor grants to the Government are unlimited rights, government purpose rights, or restricted rights. The standard license in computer software documentation conveys unlimited rights. Those rights are defined in the clause at 252.227-7014, Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation. In ~~usual~~many situations, the standard, default rights may not satisfy the Government's or the Contractor's needs or the Government may be willing to accept lesser rights in return for other consideration or to encourage competition. In those cases, a special license may be negotiated. However, while these standard, default rights are starting points of such a negotiation, the licensor is not obligated to provide the Government greater rights and the contracting officer is not required to accept lesser rights than the rights provided in the standard grant of license. The situations under which a particular grant of license applies are enumerated in paragraphs (a) through (d) of this subsection.

**

(d) *Specifically negotiated license rights.* Negotiate specific licenses when the parties agree to modify the standard, default license rights granted to the Government ~~or~~, when the Government wants to obtain rights in computer software in which it does not have sufficient rights under the standard license rights, or when the government wishes to reduce its standard license rights in return for other consideration or to encourage competition. When negotiating to obtain, relinquish, or increase the Government's rights in computer software, the contracting officer shall, in consultation with agency Intellectual Property counsel, consider using pre-approved specific licenses provided agency Intellectual Property counsel as a starting point for such negotiations, consider the impact of the special license on the Intellectual Property strategy and the planned software maintenance philosophy, anticipated time or user sharing requirements, and other factors which may have relevance for a particular procurement. If negotiating to relinquish rights in computer software documentation, consider the administrative burden associated with protecting documentation subject to restrictions from unauthorized release or disclosure. The negotiated license rights must stipulate the rights granted the Government to use, modify, reproduce, release, perform, display, or disclose the software or documentation and the extent to which the Government may authorize others to do so. Identify all negotiated rights in a license agreement made part of the contract.

17. Poor Data Item Description (DID) Alignment with Statutory/regulatory Categories Form, Fit and Function (FFF) and Operation, Maintenance, Installation, Training (OMIT)

Tension Point

There are no data acquisition documents defining data deliverables which correspond to FFF, OMIT or other specific data right categories.

Issue

The Panel discussed specific Defense Federal Acquisition Regulation Supplement (DFARS) categories of data which, regardless of funding, are licensed with unlimited rights. These categories are designed to provide enough data to maintain and procure substitute goods, but without allowing third party access to the contractor's specific trade secrets when developed exclusively at private expense. For technical data, DFARS 252.227-7013 and 252.227-7015 grant unlimited rights in FFF data and OMIT data (data necessary for operations, maintenance, installation and training purposes except for detailed manufacturing or process data). For non-commercial computer software, DFARS 252.227-7014 grants unlimited rights in computer software documentation. These terms are defined in these clauses, and have a specific contractual meaning defined in these clauses.

Discussion

The Panel noted that, in the fiscal year (FY) 2017 National Defense Authorization Act (NDAA), there are two new terms which need to be defined where the Government will have rights not based on funding:

- Interface data (technical data pertaining to an interface between an item or process and other items or processes)
- Major systems interface data (a shared boundary between a major system platform and a major system component, between major system components, or between major system platforms, defined by various physical, logical, and functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software elements; and characterized clearly in terms of form, function, and the content that flows across the interface in order to enable technological innovation, incremental improvements, integration, and interoperability.)

The Panel received comments from Government and industry about the appropriateness of changing these definitions, especially in regard to ensuring DoD depots are able to obtain necessary levels of data to perform their maintenance and sustainment functions. The Panel also received information that DoD is attempting to use these definitions in H clauses to obtain Contract Data Requirements Lists (CDRL) limited only to OMIT data, and there is DoD guidance which advises using only FFF and OMIT data where more detailed data is unavailable due to Limited Rights restrictions.

However, the Panel also received comments that such attempts to obtain CDRLs limited to OMIT data are frustrated by a conflict with requirements in the statement of work or DID which require detailed manufacturing or process data. The Panel received input that such H clauses are not necessary to order OMIT only CDRLs as long as the statement of work or DID instruct the CDRL author to remove the detailed manufacturing or process data or to only include FFF as defined in DFARS 252.227-7013 and 252.227-7015. The Panel received a comment that ASME STD Y14.24 describes types of drawings, such as control drawings, which may be exclusively FFF or OMIT data, or have very limited detailed manufacturing or process data.

The Panel is not aware of DIDs which define the format and content needed to obtain interfaces and major system interfaces needed for open architecture and modular open system approaches. As directed in the FY2017 NDAA, the Government will have specific rights in these documents once implemented in DFARS 242.227-7013, 252.227-7014, and 252.227-7015.

The Panel is not aware of any standard DIDs number, military specifications, or military standards which define CDRLs which align with these licensed rights, or use industry standard definitions which naturally align with these definitions and which would encourage competition while protecting contractor rights.

The Panel was also provided information that specific DIDs include requirements to identify rights in data, which is duplicative of (and potentially in conflict with) DFARS 252.227-7017 (with amendments after award implemented under DFARS 252.227-7013(e) and 252.227-7014(e)). Examples of such DIDs include the requirement in the Data Accession List to indicate a data rights category, as well as in the Material Data Report which has a similar requirement.

Recommendation

The Panel does not recommend any changes to 10 U.S.C. 2320 or 2321.

The Panel does not recommend any changes to the DFARS.

The Panel does recommend that the DoD create Data Item Descriptions number, military specifications, or military standards to align with the following licenses for use in competitive procurement and upgrades without contractor data rights restrictions:

- FFF data as defined in DFARS 252.227-7013 and 252.227-7015,
- OMIT data (data necessary for operations, maintenance, installation and training purposes except for detailed manufacturing or process data) as defined in DFARS 252.227-7013 & 252.227-7015.
- Computer software documentation as defined in DFARS 252.227-7014
- Interface data (technical data pertaining to an interface between an item or process and other items or processes) as will be defined in DFARS 252.227-7013, 252.227-7014 & 252.227-7015
- Major systems interface data (a shared boundary between a major system platform and a major system component, between major system components, or between major system platforms, defined by various physical, logical, and functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software elements; and '(B) is characterized clearly in terms of form, function, and the content that flows across the interface in order to enable technological innovation, incremental improvements, integration, and interoperability) as will be defined in DFARS 252.227-7013, 252.227-7014 & 252.227-7015.

For example, create a standard CDRL language for an item identification drawing: the contractor shall prepare a control drawing as defined in ASME STD Y 14.24, in which shall compromise solely of FFF and OMIT (excluding detailed manufacturing or process data) data as defined DFARS 252.227-7013 and 252.227-7015 which shall be delivered with unlimited rights. The Panel also recommends that DoD 5010.12M, MIL-STD-31000, etc., be revised to incorporate a section, including examples, of how to define and order CDRLs using the created DIDs number, military specifications, or military standards, and describe how they are used to encourage competition while protecting contractor rights in their privately developed or commercial technology.

The Panel also recommends that the existing DIDs number, military specifications, or military standards be reviewed to ensure that these document formats are not creating reporting requirements duplicate reporting requirements in a DFARS clause.

18. The Validation Process is Cumbersome and Confusing

Tension Point

The validation process is required by 10 U.S.C. 2321 and is implemented for technical data by the Defense Federal Acquisition Regulation Supplement (DFARS) 252.227-7037, and by policy is extended to noncommercial computer software, at DFARS 252.227-7019. This process provides a specific process for the Government to follow when it believes that restrictions on data delivered under the contract are inappropriate under the allocation of license rights in the contracts clauses (DFARS 252.227-7013, 252.227-7014, 252.227-7015). This process provides burdens of proof on both the Government and contractor, and specific timetables for response. The validation process is too cumbersome and confusing for practical use, which prevents Contractors and Government from getting contractual certainty on key terminology.

Issue

The Panel received comments from industry that the validation process is cumbersome. One issue is that 10 U.S.C. 2321(d)(2)(B) restricts the grounds for challenges (and effectively prevents challenges based on development funding) if the challenge is not brought within six years of the later of the data delivered or final contract payment. For complex contracts, this creates an extended deadline of perhaps decades until the contract is closed, and is inconsistent with other contractual disputes which need to be resolved within six years of claim accrual (41 U.S.C. 7103(a)(4)(A)). These industry comments indicate that the statute should be changed to limit 10 U.S.C. 2321(d)(2)(B) to only apply to six years after delivery of the data. It is noted that such a change would not affect the Government's ability to challenge on other grounds listed in 10 U.S.C. 2321(a)(2)(A).

Discussion

The Panel received a comment from industry relating to the complexity of the validation process for commercial items the licenses of which are specified in either DFARS 252.227-7015 or 252.227-7013. The commercial item definition does not require items to be developed exclusively at private expense to qualify as commercial items. Further, commerciality claims are governed by regulations outside of DFARS part 227 or 10 U.S.C. 2321, which require a presumption of development at private expense. Since the Government's rights in commercial items are not related to funding under the applicable contract clauses (DFARS 252.227-7015) unless made so under a commercial technical data license, the Government is not being improperly restricted by these clauses, even where it overcomes this presumption , unless the

commercial technical data license provides funding as a basis for such change. The existing DFARS 252.227-7037 clause does not reflect this situation.

Regarding commercial items, the Panel received an industry comment relating to 10 U.S.C. 2321(f) which requires that commercial technical data be subject to a complex presumption-switching process in which a presumption of private expense varies according to how (and at what level of the supply chain) an item is procured. The comment contended that commercial item vendors are exposed to a more complex validation scheme under DFARS 252.227-7037 and 252.227-7019 than non-commercial vendors since, in the implementation, these new requirements are copied directly into the contract clauses. This complex presumption switching is contrary to how disputes are resolved in normal commercial practice where rights are allocated according to definitions made by the parties, which may not be based on who funded the development. Moreover, commercial companies may not maintain the archives, record keeping and financial systems necessary to demonstrate development at private expense, thereby potentially rendering the presumption of development at private expense vulnerable where the Government can demonstrate funding for minor modifications or modifications of a type. The validation provision should therefore reflect the rights allocation as determined in the contract for unmodified and modified elements of the commercial item.

Industry further recommended modifying 10 U.S.C. 2320 and 2321 to exclude any mention of commercial items or, at the very least, tie the rights allocations to the contractually agreed upon categories relative to the background technology (the commercial baseline) and to the foreground technology developed under the contract. To the extent that funding is a basis for this rights allocation, the rights allocation could be the presumption that all commercial items are developed exclusively at private expense and make clear that modifications to commercial items may not be used as the basis for rebutting the presumption of development exclusively at private expense for so long as the modified item qualifies as a commercial item in accordance with 41 U.S.C. 103.

The Panel received industry comments regarding the new provision in 10 U.S.C. 2321 (d)(2)(iv), which allows challenges at any time for “fraudulently asserted use or release restriction.” The existing DFARS guidance is based on presumptions more applicable to contract breaches, whereas claims involving fraud are normally plead with particularity (see, e.g., FRCP 9(b)) and to use a clear and convincing evidence. As such, the comment suggested that, in the unique case of fraud, the DFARS guidance ensure that the contracting officers are aware of the heightened pleading and evidentiary requirements for fraud.

The Panel received industry comments regarding confusion between the data assertion list update process in DFARS 252.227-7013 and 252.227-7014, and the challenge process for delivered data in DFARS 252.227-7037 and 252.227-7019. The contractor’s ability to add new assertions to an

assertion list under DFARS 252.227-7013 and 252.227-7014 is governed by a separate process which does not affect the Government's ability to challenge the data on delivery.

The Panel received industry comments that the existing prechallenge request for information in DFARS 252.227-7013 and 252.227-7014 is problematic since the request does not require identification of specific issues to which the contractor should respond. In order to be meaningful, the comment indicated that the contracting officer should at least provide, for each challenged data item for which the contracting officer is requesting information, the factual basis for the contracting officer's issues for that piece of technical data.

The Panel also received an industry comment about the timing of the written challenge notification in DFARS 252.227-7037(e). Under this process, the contractors must respond within 60 days to support the restriction's validity on receipt of the written challenge. In contrast, the contracting officer has no time limit for issuing a written challenge after the contractor response to a pre-challenge request for information under DFARS 252.227-7037(d). According to the comment, 60 days is not an adequate time to justify an assertion where such assertions are often based on items developed years or decades earlier than the written challenge notification, which makes finding the evidence of development and financial records difficult to locate and integrate into a contractor's response. The Panel notes that the existing DFARS 252.227-7037(e)(iv)(2) does give the contracting officer discretion to extend the time period. DFARS 252.227-7019 has a similar process. Further, the contractor often will need to keep records for correcting the data under DFARS 252.246-7001, which would indicate that this issue is less acute where written challenges are presented earlier.

The Panel received comments from Government representatives that the validation process may be too cumbersome and therefore does not lead to meaningful case law. The comment did not make a specific suggestion, or indicate that other claims processes (including the Contract Disputes Act process) would be preferable. Such a change would require a change to 10 U.S.C. 2321. Further, this comment about a lack of case law is similar to that of alternative dispute resolution processes, which is analogous to the validation process. It is also unclear as to whether the timing of the validation process contributes to the lack of case law. The Panel did not reach a consensus on the advisability of changes the statute.

The Panel also was concerned about a decision based on DFARS 252.227-7019 whereby a subtier supplier was unable to appeal a contracting officer's final decision to the Armed Services Board of Contract Appeals (ASBCA). In *Appeal of Binghamton Simulator Company*, ASBCA No. 59117, 14-1 BCA ¶ 35715, 2014 WL 4355174 (2014), an ASBCA panel dismissed for lack of jurisdiction a subcontractor's dispute regarding a contracting officer's decision as to whether the Government had government purpose rights or SBIR data rights to Binghamton Simulator Company's (BSC's) "sling loads" and "hoist" software programs. The prime contractor, Leidos,

Inc. (previously known as SAIC) did not sponsor BSC's appeal. Leidos stated that BSC had never requested sponsorship of an appeal.

Under the Contract Disputes Act (CDA), only a contractor may appeal to the Board from a contracting officer's final decision. The CDA defines "contractor" as "a party to a Federal Government contract other than the Federal Government." 41 U.S.C. 7101(7). The CDA is a waiver of sovereign immunity, and as such it must be strictly construed. Parties that are not in privity of contract with the government may not avail themselves of the CDA's appeal provisions.

10 U.S.C. 2321(h), Claims, states that any claim pertaining to the validity of the asserted restriction, which is submitted in writing to a contracting officer by a contractor or subcontractor at any tier, shall be considered a claim within the meaning of chapter 71 of title 41. However, 10 U.S.C. 2321 is silent as to whether that "subcontractor at any tier" has any appeal rights. While such subtier suppliers may have remedies under the Tucker Act, the decision arguably deprives subtier suppliers of an ability to directly protect their technical data or non-commercial computer program licenses under the existing legal framework. Since 10 USC 2321 already grants an appeal right under chapter 71 of title 41, the Panel proposes modifying the term "contractor" in the CDA to include subcontractor for purposes of the validation process, while also ensuring such appeal rights apply generally for non-commercial computer software.

Recommendation

The Panel recommends changes 10 U.S.C. 2321 as attached.

The Panel also recommends changes to the DFARS to bring it into alignment with the commercial technical data license under DFARS 252.227-7015.

DFARS 227.7103-13, Government right to review, verify, challenge, and validate asserted restrictions.

(c) Challenge considerations and presumption.

(1) Requirements to initiate a challenge. Contracting officers shall have reasonable grounds to challenge the validity of an asserted restriction. Before issuing a challenge to an asserted restriction, carefully consider all available information pertaining to the assertion. Where such challenge is based on a fraudulently asserted use or release restriction, the contracting officer will consult with agency intellectual property counsel ensure such reasonable grounds include particular facts showing fraud, and clear and convincing evidence of the same. The contracting

officer shall not challenge a contractor's assertion that a commercial item was developed exclusively at private expense unless the Government can demonstrate that it contributed to development of that item and private expense was a basis for changing the Government's license rights in the technical data. The presumption does not affect the Contracting Officer's ability to challenge a restriction where the restriction is contrary to the Government's rights in the technical data licensed under DFARS 252.227-7015 or any commercial license for the technical data.

DFARS 252.227-7013, Rights in technical data—Noncommercial items.

(e) Identification and delivery of data to be furnished with restrictions on use, release, or disclosure. (1) This paragraph does not apply to restrictions based solely on copyright.

...

(4) When requested by the Contracting Officer, the Contractor shall provide sufficient information to enable the Contracting Officer to understand what is being asserted and to ensure the assertion is formatted correctly. The Contracting Officer reserves the right to add the Contractor's assertions to the Attachment and validate any listed assertion, at a later date, in accordance with the procedures of the Validation of Restrictive Markings on Technical Data clause of this contract.

A corresponding change should be made to DFARS 252.227-7014.

DFARS 252.227-7019, Validation of asserted restrictions—Computer software.

(d) Requests for information. (1) The Contracting Officer may request the Contractor to provide sufficient information to enable the Contracting Officer to evaluate the Contractor's asserted restrictions. Such information shall be based upon the records required by this clause or other information reasonably available to the Contractor. The Contracting Officer's request should include the specific item or items of computer software being evaluated, and any factual basis which might affect the Contractor's restriction.

A similar change should be made to DFARS 252.227-7037.

10 U.S. Code § 2321 - Validation of proprietary data restrictions

(a) Contracts Covered by Section.—

This section applies to any contract for supplies or services entered into by the Department of Defense that includes provisions for the delivery of technical data or noncommercial computer software.

(b) Contractor Justification for Restrictions.—

A contract subject to this section shall provide that a contractor under the contract and any subcontractor under the contract at any tier shall be prepared to furnish to the contracting officer a written justification for any use or release restriction (as defined in subsection (i)) asserted by the contractor or subcontractor.

(c) Review of Restrictions.—

(1) The Secretary of Defense shall ensure that there is a thorough review of the appropriateness of any use or release restriction asserted with respect to technical data or noncommercial computer software by a contractor or subcontractor at any tier under a contract subject to this section.

(2) The review of an asserted use or release restriction under paragraph (1) shall be conducted before the end of the three-year period beginning on the later of—

(A) the date on which final payment is made on the contract under which the technical data or noncommercial computer software is required to be delivered; or

(B) the date on which the technical data or noncommercial computer software is delivered under the contract.

(d) Challenges to Restrictions.—

(1) The Secretary of Defense may challenge a use or release restriction asserted with respect to technical data or noncommercial computer software by a contractor or subcontractor at any tier under a contract subject to this section if the Secretary finds that—

(A) reasonable grounds exist to question the current validity of the asserted restriction; and

(B) the continued adherence by the United States to the asserted restriction would make it impracticable to procure the item to which the technical data or noncommercial computer software pertain competitively at a later time.

(2)

(A) A challenge to a use or release restriction asserted by the contractor in accordance with applicable regulations may not be made under paragraph (1) after the end of the six-year period described in subparagraph (B) unless the technical data or noncommercial computer software involved—

(i) are publicly available;

- (ii) have been furnished to the United States without restriction;
- (iii) have been otherwise made available without restriction; or
- (iv) are the subject of a fraudulently asserted use or release restriction.

(B) The six-year period referred to in subparagraph (A) is the six-year period beginning on the later of—

- (i) the date on which the final payment item (other than technical data or noncommercial computer software) is ~~made accepted~~ on the contract under which the technical data or noncommercial computer software are required to be delivered; or
- (ii) the date on which the technical data or noncommercial computer software are delivered under the contract.

(3) If the Secretary challenges an asserted use or release restriction under paragraph (1), the Secretary shall provide written notice of the challenge to the contractor or subcontractor asserting the restriction. Any such notice shall—

- (A) state the specific grounds for challenging the asserted restriction;
- (B) require a response within 60 days justifying the current validity of the asserted restriction; and
- (C) state that evidence of a justification described in paragraph (4) may be submitted.

(4) It is a justification of an asserted use or release restriction challenged under paragraph (1) that, within the three-year period preceding the challenge to the restriction, the Department of Defense validated a restriction identical to the asserted restriction if—

- (A) such validation occurred after a challenge to the validated restriction under this subsection; and
- (B) the validated restriction was asserted by the same contractor or subcontractor (or a licensee of such contractor or subcontractor).

(e) Time for Contractors to Submit Justifications.—

If a contractor or subcontractor asserting a use or release restriction submits to the contracting officer a written request, showing the need for additional time to comply with the requirement to justify the current validity of the asserted restriction, additional time to adequately permit the submission of such justification shall be provided by the contracting officer as appropriate. If a party asserting a restriction receives notices of challenges to restrictions on technical data or noncommercial computer software from more than one contracting officer, and notifies each contracting officer of the existence of more than one challenge, the contracting officer initiating the first in time challenge, after consultation with the party asserting the restriction and the other contracting officers, shall formulate a schedule of responses to each of the challenges that will afford the party asserting the restriction with an equitable opportunity to respond to each such challenge.

(f) Presumption of Development Exclusively at Private Expense.—

(1) Except as provided in paragraph (2), in the case of a challenge to a use or release restriction that is asserted with respect to technical data of a contractor or subcontractor under a contract for commercial items, the contracting officer shall presume that the contractor or subcontractor has justified the restriction on the basis that the item was developed exclusively at private expense, whether or not the contractor or subcontractor submits a justification in response to the notice provided pursuant to subsection (d)(3). In such a case, the challenge to the use or release restriction may be sustained only if information provided by the Department of Defense demonstrates that the item was not developed exclusively at private expense.

(2) In the case of a challenge to a use or release restriction that is asserted with respect to technical data of a contractor or subcontractor for a major system or a subsystem or component thereof on the basis that the major weapon system, subsystem, or component was developed exclusively at private expense—

(A) the presumption in paragraph (1) shall apply—

(i) with regard to a commercial subsystem or component of a major system, if the major system was acquired as a commercial item in accordance with section 2379(a) of this title;

(ii) with regard to a component of a subsystem, if the subsystem was acquired as a commercial item in accordance with section 2379(b) of this title; and

(iii) with regard to any other component, if the component is a commercially available off-the-shelf item or a commercially available off-the-shelf item with modifications of a type customarily available in the commercial marketplace or minor modifications made to meet Federal Government requirements; and

(B) in all other cases, the challenge to the use or release restriction shall be sustained unless information provided by the contractor or subcontractor demonstrates that the item was developed exclusively at private expense.

(g) Decision by Contracting Officer.—

(1) Upon a failure by the contractor or subcontractor to submit any response under subsection (d)(3), the contracting officer shall issue a decision pertaining to the validity of the asserted restriction.

(2) After review of any justification submitted in response to the notice provided pursuant to subsection (d)(3), the contracting officer shall, within 60 days of receipt of any justification submitted, issue a decision or notify the party asserting the restriction of the time within which a decision will be issued.

(h) Claims.—

Any appeal by a contractor or subcontractor of a decision under (g) shall be considered a claim within the meaning of chapter 71 of title 41, and the contractor or subcontractor asserting the restriction which is the subject of the decision under (g) shall be considered a “contractor” within

~~the meaning of chapter 71 of title 41. If a claim pertaining to the validity of the asserted restriction is submitted in writing to a contracting officer by a contractor or subcontractor at any tier, such claim shall be considered a claim within the meaning of chapter 71 of title 41.~~

(i) Rights and Liability Upon Final Disposition.—

(1) If, upon final disposition, the contracting officer's challenge to the use or release restriction is sustained—

- (A) the restriction shall be cancelled; and
- (B) if the asserted restriction is found not to be substantially justified, the contractor or subcontractor asserting the restriction shall be liable to the United States for payment of the cost to the United States of reviewing the asserted restriction and the fees and other expenses (as defined in section 2412(d)(2)(A) of title 28) incurred by the United States in challenging the asserted restriction, unless special circumstances would make such payment unjust.

(2) If, upon final disposition, the contracting officer's challenge to the use or release restriction is not sustained—

- (A) the United States shall continue to be bound by the restriction; and
- (B) the United States shall be liable for payment to the party asserting the restriction for fees and other expenses (as defined in section 2412(d)(2)(A) of title 28) incurred by the party asserting the restriction in defending the asserted restriction if the challenge by the United States is found not to be made in good faith.

(j) Use or Release Restriction Defined.—In this section, the term “use or release restriction”, with respect to technical data or noncommercial computer software delivered to the United States under a contract subject to this section, means a restriction by the contractor or subcontractor on the right of the United States—

- (1) to use such technical data or noncommercial computer software; or
- (2) to release or disclose such technical data or noncommercial computer software to persons outside the Government or permit the use of such technical data or noncommercial computer software by persons outside the Government.

19 Mandatory flow-down (commercial subs and suppliers) (Majority Position)

Tension Point

Clarify Statutory Requirements and Eliminate Mandatory Flow-Downs for Commercial Items.

Discussion

The panel has discussed whether or not it is in the best interest of the government for the DoD to apply and flow-down 10 USC 2320 and 2321 (the “technical data statutes”) to commercial items.

Legislative History

The panel has discussed the extent to which the technical data statutes apply to all commercial items procured at the contract or subcontract level. Enclosure 1 includes a discussion of the applicable legislative history. Industry and government panelists have differing views regarding congressional intent. Notwithstanding, the panel has reached consensus on certain statutory and regulatory recommendations, described below, that are intended to clarify statutory applicability, alleviate the regulatory burden on the commercial supply chain, achieve contracting efficiencies, and, at the same time, hold prime contractors and higher-tier subcontractors accountable for meeting prime contract requirements.

Applicability and Flow-Down of the Technical Data Statutes to COTS Items and “Subcontracts”

In 2011, the DAR Council amended the DFARS to mandate the flow-down of three DFARS data rights clauses to commercial subcontractors and suppliers: DFARS 252.227-7013, Rights in Technical Data--Noncommercial Items¹; DFARS 252.227-7015, Technical Data--Commercial Items, and DFARS 252.227-7037, Validation of Restrictive Markings on Technical Data.

DFARS 252.227-7015 and DFARS 252.227-7037 are mandatory flow-downs to *all* “subcontractors” and “suppliers” which deliver commercial technical data that will in turn be delivered to the DoD (including COTS suppliers and other suppliers operating under separate commercial supply agreements that are not identifiable to any prime contract). Some industry panelists have expressed concern that mandating flow-down to COTS suppliers may impede DoD’s access to commercial items. Commercial vendors may be unwilling to accept DoD-unique data rights clauses that introduce IP risk or require commercial vendors to grant license rights in a scope different from the licenses granted in the commercial marketplace.

Some industry panelists and the Aerospace Industries Association (AIA) have also expressed concerns regarding the mandatory flow-down of the clauses discussed above to “suppliers” operating under separate supply chain agreements or “other contractual instruments” that are

¹ DFARS 252.227-7013 is a mandatory flow-down, only to the extent the commercial item will have been developed in any part with government funding.

not identifiable to any specific prime contract, sale or order. Such supply chain agreements are not “subcontracts” awarded pursuant to a specific prime contract. They are often used to procure commodities or COTS items on a long-term basis (generally ranging from a few years to 20 years) and are often placed for the purposes of acquiring supplies to support company-wide or division-wide operations, to develop multiple product lines, to support commercial production rates or for spares inventory.

Sourcing decisions for such commercial supply chain agreements are generally made before Government contract requirements (for commercial items) are even known to the prime contractor. And most importantly, *such commercial supply chain agreements enable the government to benefit from economies of scale and pricing efficiencies achieved only in the commercial marketplace*. Commercial suppliers operating under such agreements have agreed to commercial pricing prior to the award of any prime contract, and such commercial prices are not based on the acceptance of future DoD flow-down clauses, which establish DoD-unique license rights, assertion requirements, marking requirements, records-keeping requirements or supplier monitoring requirements.

To illustrate the significant cost and schedule impacts that such flow-down requirements could have on a major system or weapon system, the Council of Defense and Space Industry Associations (CODSIA), in its public comments in response to DFARS Case 2012-D022, stated that with regard to one major defense acquisition program, there are over 500 commercial suppliers at the first-tier of the commercial supply chain, with almost 25% of such commercial suppliers qualifying as small businesses. CODSIA noted that it is likely that the total number of commercial suppliers at all tiers for this program exceeds 1000.

Some industry panelists are also concerned about the inflexibility of mandatory flow-down requirements because buying commands are generally unwilling to negotiate deviations to mandatory flow-down requirements, or are otherwise unwilling to undertake the effort required to pursue individual deviations from DPAP pursuant to DFARS 201.402(1)(ii) (DPAP is the approval authority within DoD for any individual or class deviation from DFARS Subpart 227.4, Rights in Data and Copyrights). In cases where prime contractors attempt to negotiate flow-down language, some customers have expected prime contractors to offer concessions in exchange for negotiating deviations, *even though eliminating flow-down requirements may lead to lower prices paid for by the Government*.

In the referenced CODSIA public comments, CODSIA encouraged the DAR Council to explore congressional intent regarding the applicability and flow-down of laws and regulations to commercial supply chain agreements or other “contractual instruments” which are not identifiable to, or awarded pursuant to, Government prime contracts. CODSIA noted that 41 USC 1906 and 1907 use only the terms “contract” and “subcontract,” with the latter term generally used in practice to refer to contractual relationships established for the purposes of fulfilling prime contract requirements. The panel notes that the technical data statutes also use only the terms “contract” and “subcontract” – and not “supplier.”

Most recently, Congress addressed the need to distinguish between subcontractors and suppliers in Section 874 of the FY17 NDAA, discussed in Enclosure 1.

The panel recommends the establishment of a statement of policy for the acquisition of COTS items in 10 USC 2320, which would not be subject to the 10 USC 2321 validation

procedures. The panel recommends establishing uniform definition of “subcontract” in policy that excludes the procurement of commodities or commercially available off-the-shelf products that are intended for use in the performance of multiple contracts with the Department of Defense and other parties and are not identifiable to any particular contract.

In regulatory implementation, the panel recommends deletion of references to “suppliers” and “other contractual instruments” to align flow-down requirements with Section 874 of the FY17 NDAA and Section 820 of the FY18 NDAA.

Flow-Down of DFARS 252.227-7013 and DFARS 252.227-7015 to All Other Commercial Items Procured at the Subcontract Level

The panel discussed the need to provide flexibility to prime contractors and higher-tier subcontractors in negotiating data rights clauses for technical data pertaining to other commercial items, such as items that will undergo “minor” or “of a type” modifications. The panel recommends the following changes to provide such flexibility:

- Eliminate mandatory data rights flow-down requirements for all other commercial items, while holding prime contractors and higher-tier subcontractors accountable for meeting the technical data delivery and license rights requirements in their respective contracts or subcontracts.
- The panel also discussed the continued importance of requiring contractors and higher-tier subcontractors to ensure that subcontractors benefit from the rights and protections under 10 USC 2320 and 2321. In furtherance of this objective, the panel recommends adding new regulatory language that would enable subcontractors to “opt in” to data rights clause flow-downs on a case-by-case basis.
- Add new DFARS policy language encouraging the negotiation of customized commercial licenses that balance the needs of the parties.

Applicability of the Validation Procedures at 10 USC 2321 to All Other Commercial Items

Commercial items do not have to be developed exclusively at private expense to meet the commercial item definition at 41 USC 103 (as referenced in 10 USC 2376). The source of development funding is *only* relevant in the case of “nondevelopmental items”² (see 41 USC 103 (8)).

It is possible that a non-COTS commercial item initially developed at Government expense could be subsequently sold or offered for sale to the Government as a commercial item. In such a case, the Government could use the applicable prior development contracts to prove that the item, or portions thereto, was developed at Government expense, and the technical data statutes should apply and flow-down to the portions of the item that were initially developed at Government expense.

² For a nondevelopmental item to qualify as a commercial item, the procuring agency must determine, in accordance with conditions in the Federal Acquisition Regulation, that the item was developed exclusively at private expense and has been sold in substantial quantities, on a competitive basis, to multiple State and local governments.

Industry panelists have indicated that Government customers often equate all modifications with development. Such positions are inconsistent with the intellectual property white paper entitled, "DoD, Innovation, and Intellectual Property in Commercial & Proprietary Technologies," which was published by DoD in November of 2015 in support of its efforts to cultivate relationships with commercial companies and non-traditional contractors, such as those in Silicon Valley.

The white paper states that, "... *only those modifications that rise to the level of a new technology "development" could affect the standard license rights granted to DoD in the newly developed modification...*"

There is currently no guidance in the regulations regarding how to determine whether modifications rise to the level of new technology development. The current regulatory framework for proving private expense development of commercial items shifts too much IP risk for commercial companies to contract or subcontract performance and beyond, as a result of applicability of the validation procedures. A prospective approach is needed to determine whether modifications will rise to the level of new technology development. A prospective approach will ensure that commercial companies sufficiently understand the IP risks associated with modifying their commercial items to meet unique DoD requirements, up front, and may also mitigate disputes that may arise during contract performance. To prospectively address this issue, the panel recommends the establishment of DFARS policy and associated clause language requiring the parties to specify which portions of a commercial item, or which technical data, the -7037 clause would apply to.

Major System Interfaces

Section 809 of the FY17 NDAA established government purpose rights (GPR) for major system interfaces (MSIs) developed exclusively at private expense, to implement Modular Open System Approaches (MOSA). Industry panelists expressed concerns about the applicability of these provisions to commercial items, which would increase the regulatory burden on the commercial supply chain. Industry panelists also expressed concern that commercial companies may refuse to do business with the DoD or deliver technical data or computer software, due to their refusal to deliver major system interfaces with GPR.

The panel's recommendations for statutory treatment of COTS items alleviates industry's concern for COTS. For all other commercial items, the panel discussed that paragraph (a)(2)(G) of 10 USC 2320 provides flexibility to DoD to negotiate a different set of rights (other than GPR) in privately developed interfaces when it's in the best interest of the government to do so.

Recommendations

Statutory Changes:

Amend 10 USC 2320 by adding new (a)(2)(J) as follows:

(J) Notwithstanding subparagraphs (A) through (G), in the case of a commercially available off-the-shelf item, as defined in section 104 of title 41—

(i) the United States shall acquire only the technical data, and the rights in such technical data, that are customarily provided to the public, unless such technical data or rights are inconsistent with federal law or do not satisfy the needs of the United States; and

(ii) the Secretary of Defense shall negotiate with the contractor or subcontractor for any additional technical data or rights necessary to satisfy the needs of the United States.

Amend 10 USC 2321 as shown below. The Panel recommends deletion of (f)(2) in order to streamline the validation process because the statutory presumptions are unwieldy and difficult to apply in practice.

(a) This section applies to any contract for supplies or services (except for commercially available off-the-shelf items, as defined in section 104 of Title 41) entered into by the Department of Defense that includes provisions for the delivery of technical data. In the case of all other commercial items, this section shall apply except to the extent specified in the contract in accordance with criteria specified by the Secretary to balance the respective interests of the United States and the contractor or subcontractor.

...

(f) Presumption of Development Exclusively at Private Expense.—

~~(1) Except as provided in paragraph (2),~~ In the case of a challenge to a use or release restriction that is asserted with respect to technical data of a contractor or subcontractor under a contract for commercial items (other than commercially available off-the-shelf items), the contracting officer shall presume that the contractor or subcontractor has justified the restriction on the basis that the item was developed exclusively at private expense, whether or not the contractor or subcontractor submits a justification in response to the notice provided pursuant to subsection (d)(3). In such a case, the challenge to the use or release restriction may be sustained only if information provided by the Department of Defense demonstrates that the item was not developed exclusively at private expense.

~~(2) In the case of a challenge to a use or release restriction that is asserted with respect to technical data of a contractor or subcontractor for a major system or a subsystem or component thereof on the basis that the major weapon system, subsystem, or component was developed exclusively at private expense—~~

~~A) the presumption in paragraph (1) shall apply—~~

~~(i) with regard to a commercial subsystem or component of a major system, if the major system was acquired as a commercial item in accordance with section 2379(a) of this title;~~

~~(ii) with regard to a component of a subsystem, if the subsystem was acquired as a commercial item in accordance with section 2379(b) of this title and~~

~~(iii) with regard to any other component, if the component is a commercially available off-the-shelf item or a commercially available off-the-shelf item with modifications of a type customarily available in the commercial marketplace or minor modifications made to meet Federal Government requirements; and~~

~~(B)~~

~~in all other cases, the challenge to the use or release restriction shall be sustained unless information provided by the contractor or subcontractor demonstrates that the item was developed exclusively at private expense.~~

Regulatory changes:

1. The panel recommends the issuance of MOSA guidance regarding situations where the Secretary of Defense may consider alternative licensing solutions for MSIs, such as for commercial items (other than COTS items).
2. The panel recommends that the criteria established pursuant to the proposed revisions to 10 USC 2321 consider the issues raised in this paper and Tension Paper 14
3. The panel recommends establishing uniform definition of “subcontract” in policy that excludes the procurement of commodities or commercially available off-the-shelf products that are intended for use in the performance of multiple contracts with the Department of Defense and other parties and are not identifiable to any particular contract.
4. Remove “supplier” and “other contractual instruments” from the flow-down requirements of 252.227-7013, 7015, and 7037.
5. Eliminate mandatory data rights flow-down requirements for all other commercial items, while holding prime contractors and higher-tier subcontractors accountable for meeting the technical data delivery and license rights requirements in their respective contracts or subcontracts.
6. The Panel recommends adding new regulatory language that would enable subcontractors to “opt in” to data rights clause flow-downs on a case-by-case basis.
7. Add new DFARS policy language encouraging the negotiation of customized commercial licenses that balance the needs of the parties.
8. The Panel recommends the establishment of DFARS policy and associated clause language enabling the parties to specify which portions of a commercial item, or which technical data, to which the -7037 clause would apply. An example would be the alternative clause structure found in FAR 52.227-3.

Enclosure 1: Legislative and Regulatory History:

I. Presumption of Development Exclusively at Private Expense and Congressional Intent re the Applicability of the Technical Data Statutes to Commercial Items

The Federal Acquisition Streamlining Act of 1994 (“FASA”) (P. L. 103-355) set forth statutory changes intended to reduce barriers to the acquisition of commercial items, including: (1) the establishment of the commercial item definition (now codified at 41 USC 103); (2) a statutory preference for the acquisition of commercial items (codified at 10 USC 2377); (3) the establishment of a presumption of development exclusively at private expense for commercial items (codified in 10 USC 2321(f)) and (4) a requirement for the FAR (and by extension, the DFARS) to include lists of provisions of law that are *inapplicable* to “contracts” and “subcontracts” for commercial items (now codified in 41 USC 1906³).

The Conference Report accompanying FASA included the following:

“Presumption that technical data under contracts for commercial items are developed exclusively at private expense (sec. 8106)

The House amendment contained a provision that would exempt commercial items from 10 U.S.C. 2320 (technical data) and 2321 (validation of proprietary data restrictions).

The Senate bill contained no similar provision.

The Senate recedes with an amendment which would provide that, for the purposes of technical data provisions in 10 U.S.C. 2320 and 10 U.S.C. 2321, a commercial item will be presumed to have been developed exclusively at private expense unless a federal agency can document that the item was developed, in whole or in part, at federal government expense.”

The conferees were concerned that a blanket waiver from these statutes could prevent the federal government from obtaining technical data rights on items developed with public funds. The conference approach would have the effect of exempting commercial items from the requirement to provide technical data (other than data on form, fit and function), unless the government can prove that an item was developed at government expense.”

In Section 802(b) of the FY 2007 National Defense Authorization Act (NDAA) (P.L. 109-364), Congress amended § 2321(f) to eliminate the FASA presumption of development at private expense for commercial items in the case of a major system or a subsystem or component thereof. The FASA presumption was partially restored the following year for COTS items (see Section 815(a)(2) of the FY 2008 NDAA (P.L. 110-181)).

In Section 813 of the FY 2016 NDAA, Congress again amended 10 USC 2321 to clarify the presumption language. The conference report accompanying the NDAA stated:

“Rights in technical data (sec. 813)

³ Although currently codified at 41 USC 1906 as a result of [Pub. L. 111-350](#), this section was originally codified at 41 USC 430.

The Senate amendment contained a provision (sec. 825) that would clarify procedures for the validation of rights in technical data for subsystems and components of major weapon systems; and establish a government-industry advisory panel to review sections 2320 and 2321 of title 10, United States Code.

The House bill contained no similar provision.

The House recedes.”

The Senate report accompanying the Senate version of the FY 2016 NDAA also stated:

“Rights in technical data (sec. 825)

The committee recommends a provision that: (1) Would clarify procedures for the validation of rights in technical data for subsystems and components of major weapon systems; and (2) establish a government-industry advisory panel on rights in technical data.

The provision would amend section 2321 of title 10, United States Code, that establishes procedures for the validation of rights in technical data. Subsection (f) of this section, added by the Federal Acquisition Streamlining Act of 1994 (Public Law 103–355), endeavored to protect intellectual property rights in commercial items by adding a presumption that commercial items are developed exclusively at private expense. Because almost all major weapon systems are developed at government expense, section 802 of the John Warner National Defense Authorization Act for Fiscal Year 2007 (Public Law 109–364) added an exception to the presumption in subsection (f) in the case of items other than commercially available off-the-shelf (COTS) items that are included in major weapon systems.

The exception for major weapon systems in subsection 2321(f) has created two potential problem areas. First, although almost all major weapon systems are developed at government expense, a few major weapon systems and subsystems of major weapon systems are purchased as commercial items—for example, modified civilian aircraft that are purchased for military uses. Section 2321(f) requires the contractor to demonstrate that components of weapon systems were developed at private expense even in the case of commercial-derivative aircraft, commercial-derivative engines, and other weapon systems and subsystems that are purchased as commercial items.

Second, although subsection 2321(f) includes an exception for COTS items that are included in major weapon systems, this exception does not apply if the COTS item is modified in any way for government use. Consequently, if the government insists on a minor modification of a COTS item for the purpose of including it in a weapon system, the burden will fall on the contractor to demonstrate that the item was developed exclusively at private expense. The provision recommended by the committee would address these problems by clarifying that the presumption that a commercial item was developed exclusively at private expense applies in the case of: (1) A component of a weapon system or subsystem that was acquired as a commercial item; and (2) any other component that is a COTS item or a COTS item with modifications of a type customarily available in the commercial market place or minor modifications made to meet government requirements.”

II. Listing Provisions of Law Inapplicable to Commercial Items

FASA established a requirement for the FAR (and by extension, the DFARS) to include lists of provisions of law that are *inapplicable* to “contracts” and “subcontracts” for commercial items (see 41 USC 1906). Provisions of law that are eligible for exemption from applicability to commercial items are those that set forth policies, procedures, requirements, or restrictions for the procurement of property or services by the Government, *except* for any provision of law that: (1) provides for criminal or civil penalties; or (2) specifically refers to 41 USC 1906 and provides that, notwithstanding 41 USC 1906, it shall be applicable to contracts or subcontracts for the procurement of commercial items (see 41 USC 1906(d)).

Two years after FASA was enacted, Congress expanded on FASA reforms in the FY 1996 NDAA to make it easier to buy “commercially available off-the-shelf” (COTS) items, a subset of commercial items that must be sold *in substantial quantities* in the commercial marketplace and offered to the Government – *without modification* – in the same form in which they are sold in the commercial marketplace (see 41 USC 104). The FY 1996 NDAA required the FAR (and DFARS) to list additional provisions of law – in addition to those listed as inapplicable to all other commercial items pursuant to 41 USC 1906 – that are inapplicable to contracts and subcontracts for the acquisition of COTS items (see 41 USC 1907⁴).

The current FAR and DFARS lists of provisions of law required by 41 USC 1906 and 1907 are: FAR 12.503 (contracts for commercial items); FAR 12.504 (subcontracts for commercial items); FAR 12.505 (COTS items); DFARS 212.503 (contracts for commercial items); DFARS 212.504 (subcontracts for commercial items) and DFARS 212.505 (COTS items). Pursuant to 41 USC 1906(c)(2), a covered provision of law “shall be included” on the DFARS 212.504 list of provisions of law that are inapplicable to subcontracts for the acquisition of commercial items *unless* the DAR Council “makes a written determination that it would not be in the best interest of the Federal Government to exempt subcontracts under a contract for the procurement of commercial items from the applicability of the provision.” 41 USC 1907(a)(2) establishes the same requirements for the acquisition of COTS items.

From 1995 until 2011, DFARS 212.504 exempted the technical data statutes from applicability to subcontracts for commercial items. DoD did not apply the statutes to subcontracts for commercial items until the issuance of the final rule implementing the FY 2007 and 2008 NDAs (see DFARS Case 2007-D003, “Presumption of Development Exclusively at Private Expense,” issued on 20 September 2011). At that time, DoD modified DFARS 212.504 to remove the technical data statutes from the DFARS 212.504 exclusionary list. In its final rulemaking, the DAR Council said that “the decision to remove these statutes from the list is based on the appropriate statutory determinations that doing so is in the best interest of the Government.”

In the final rule, the DAR Council also added three mandatory flow-down clauses that levy DoD-unique requirements on commercial subcontractors and suppliers: DFARS 252.227-7013, Rights in Technical Data--Noncommercial Items; DFARS 252.227-7015, Technical Data--Commercial Items, and DFARS 252.227-7037, Validation of Restrictive Markings on Technical Data.

⁴ Although currently codified at 41 USC 1907 as a result of [Pub. L. 111-350](#), this section was originally codified at 41 USC 431.

In Section 874 of the FY17 NDAA, Congress established additional requirements beyond 41 USC 1906 and 1907 that apply to defense-unique statutes and other DFARS contract clauses. Section 874(a) amended 10 USC 2375 to address the applicability of defense-unique statutes and other DFARS contract clauses to contracts and subcontracts for the acquisition of commercial items and COTS items.

Section 874 was based on Section 861 of the Senate version of the F7 17 NDAA. The Senate Report for Section 861 states:

"The committee recommends a provision that would amend section 2375 of title 10, United States Code, to require the establishment of a list in the Defense Federal Acquisition Regulation Supplement of inapplicable defense-unique statutes to contracts for commercial items and commercial-available off-the-shelf items. These would be in addition to those inapplicable government-wide statutes currently listed in the Federal Acquisition Regulation (FAR) pursuant to section 1906(b) of title 41, United States Code.

The committee is concerned by the growing number of government-unique contract clauses that are now required for FAR Part 12 commercial contracts. By industry estimates these clauses have grown since the mid-1990s from 13 to 63, and in some cases over 80, government-unique contract clauses today. With these requirements come additional costs and regulatory burden ultimately paid by the taxpayer while each added new clause limits the pool of potential commercial companies willing to act as defense suppliers. This limits the potential competition, innovation, and creativity that is necessary to reduce costs to the taxpayer and deliver cutting-edge equipment to the men and women of the armed forces. The committee intends that this provision be used by the Department of Defense to reduce unnecessary requirements on contractors providing commercial items that are identified in the report required by section 854 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109–163)."

Applicability of the Technical Data Statutes to "Subcontractors" and "Suppliers"

Section 874(a) of the FY17 NDAA also amended 10 USC 2375 to address the applicability of defense-unique statutes to contracts and subcontracts for commercial items. The new section (c)(3) of 10 USC 2375 expanded on the 41 USC 1906 definition of "subcontract" as follows (emphases added):

"(3) In this subsection, the term 'subcontract' includes a transfer of commercial items between divisions, subsidiaries, or affiliates of a contractor or subcontractor. The term does not include agreements entered into by a contractor for the supply of commodities that are intended for use in the performance of multiple contracts with the Department of Defense and other parties and are not identifiable to any particular contract."

Section 874(b) of the FY17 NDAA also established limitations on the extent to which the DFARS can mandate the applicability and flow-down of contract clauses that are not based in statute or executive order to contracts or subcontracts for the acquisition of commercial items or COTS items. Section 874(b) also defines the term "subcontract" in the same way it is defined in the amendments to 10 USC 2375.

Minority Report

19 Mandatory flow-down (commercial subs and suppliers)

(Minority Position)

Authors: Elliot Branch, Joseph Gordon, Roger Hamerlinck, Theodora Hancock, Charles Harris

Proposal

Seven of the twelve panel members, i.e., six industry panel members and one Government panel member (hereinafter “Majority members”) suggested a legislative proposal that would amend 10 USC 2320(a)(2)(J) to indirectly eliminate mandatory flow-down requirements for commercially available off-the-shelf items (COTS) and require negotiations for data rights for COTS items only. Another legislative proposal would amend 10 USC 2321(a) in two ways: by eliminating validation for COTS items and allowing the validation scheme for commercial items to vary from contract to contract. A final legislative proposal would amend 10 USC 2321 by deleting paragraph (f)(2). The remaining five panel members, all from the Government, (hereinafter “Minority members”) provide this Minority Position regarding the Majority members proposal.

Industry panel members provided examples of commodity contracts (e.g., contracts for nuts, bolts, rivets, basic semiconductor chips, capacitors) and commercially-available off-the shelf items (hereinafter “COTS”) and the difficulties posed by mandatory flow-down provisions to prime contractors. Commodity contracts buy raw and basic materials by the thousands and orders may be placed years in advance of a Government contract. Government panel members agreed that those administrative burdens to prime contractors should be removed for commodities and COTS items. The industry members insisted that their example of COTS items burdens should apply to all commercial items regarding the validation scheme under 10 USC 2321.

Minority Proposed Compromise: The Minority members agree that unnecessary administrative burdens can and should be addressed during the rulemaking process.

There is no need for statutory changes, when rulemaking will suffice. Additionally, any rulemaking should be narrowly tailored to address the specific problem of whether to uniformly apply the data rights validation scheme for all commercial items contracts.

Discussion

The Panel members note that the only consensus the Panel has reached is that industry has concerns about this practice. If the current statutory balance for validation of data rights assertions is so onerous that it cannot be applied uniformly across the supply chain, then the Majority members should focus on re-calibrating that balance consistent with the Panel's congressional mandate during the rulemaking process.

The Majority members encourage the Government to abandon a uniform approach for data rights validation for any commercial item. The supposed better practice is to make data rights validation a case-by-case determination that excludes some vendors, lets others "opt in," and leaves the rest entirely up to the discretion of the parties. No examples are provided to illustrate why this hodgepodge approach could be a better practice or would lead to more cost-effective re-procurement, sustainment, or related activities. Again, the Majority member position is not supported by any evidence.

This consternation about flow-down is presented from concerns about commodities and commercially available off-the-shelf items. There is no great concern in the Defense Department or Congress about the prices being paid for these widely available goods. That's not so true with the nebulous "commercial items" the Majority members sweep in among their recommendations near the end. There the problem, as shown by the legislative history, is ensuring the Defense Department remains protected when an item the Defense Department funded is re-characterized from being noncommercial to commercial. Those interests regarding taxpayer and warfighter funding will be more difficult to protect now if this Majority member recommendation is taken. With commodities and commercially available off-the-shelf items, none of the Majority members have shown that the Defense Department is paying excessive amounts due to requirements for mandatory flow-down. This is evidence of just how misplaced the Majority member's attention has been. Rather than delve into how best to promote the use of innovative products and new technologies that are relevant to the missions of the Department of Defense, the Panel has become enamored with irrelevant side issues.

The Majority members wish to "clarify" how the law should be read for purposes of validating data rights assertions for commercial items. The Majority members conclude that it is more equitable for the Defense Department to bear the burden of proof for how commercial items are funded. This recommendation is made despite Congress' expressed concerns and prior legislative changes aimed at changing a practice that did anything but lead to cost-effective sustainment. For purposes of data rights validation, the Defense Department must carry this burden before the validation requirement can be levied. According to the Majority members, only after carrying this impossible burden can the Defense Department ask for contract terms to be consistently applied through the supply chain. The Defense Department is at an extreme informational disadvantage about the items industry proposes for sale, particularly at the time of contract award. If this practice is supposed to lead to greater accountability at the prime contractor level, the Majority members do not explain. In the view of the majority of the Government members, all it will do is provide prime contractors an excuse for non-performance regarding technical data rights needed by the warfighter. And in that, only the Defense Department's needs will not be met.

PRESUMPTION OF DEVELOPMENT EXCLUSIVELY AT PRIVATE EXPENSE

It is unclear why the Majority members decided to place in this paper a statutory recommendation to delete 10 USC 2321(f)(2) regarding varying presumptions of development exclusively at private expense. Nonetheless, the recommendation is a good one as the statutory

scheme at (f)(2) is difficult to follow and more difficult to implement regarding the applicability of the various statutory presumptions.

CASE-BY-CASE APPLICATION OF DATA RIGHTS VALIDATION STATUTE REGARDING COTS ITEMS

The Majority members propose a final sentence to 10 USC 2321(a) to allow the applicability of the validation statute, which protects the interests of the warfighter and the taxpayer, to be altered or removed on a case-by-case basis. The Panel members acknowledge that a non-COTS commercial item initially developed at Government expense could be subsequently sold or offered for sale to the Government as a commercial item. In other words, an item fully funded by the Government might later be re-characterized as a commercial item and the Government would lose the benefit of its funding with respect to intellectual property rights unless the Government meticulously maintains the relevant contract documents in order to challenge the re-characterization. Further, industry supports this rebuttable presumption, even though it may result in Government funding being subsequently treated as industry funding. The Panel members want to incentivize industry to make investments in new technologies. It is not at all clear that adding more complexity to these already complex rules would spur industry investment. To the contrary, industry may be incentivized to utilize more clever lawyering or accounting, e.g., to use all Government funding to develop dual-use technologies. At some point commercial sales of that fully-Government funded technology would trigger a re-characterization, so the Government would lose its rights in that fully-Government funded technology unless the Government somehow tracked the industry product and maintained the related-financial records. It is unclear how this lawyering or accounting-based windfall to industry is a fair and equitable resolution of the tension point regarding development versus adaptation of technology.

The Minority members prefer statutory changes that incentivize industry to provide technically superior products or more affordable products. The Minority members see no value in rewarding industry for creative lawyering or creative accounting. Statutory changes such as case-by-case application of commercial item status (re-characterization addressed above), case-by-case applicability of deferred ordering, or case-by-case applicability of the data rights validation statute, reward creative lawyering or creative accounting, in our view, and do not bring better, more affordable capabilities to the warfighter. To the contrary, the Department of Defense may be vendor-locked and forced into a sole source position for decades, which is to the detriment of the taxpayer (due to lack of cost control) and to the detriment of the warfighter (due to lack to better or more affordable technology).

This end result does not serve the interests of the warfighter. These Majority Report recommendations do not serve the desires of Congress.

Recommendation:

We concur with the Majority members recommendation to delete paragraph (f)(2) of 10 USC 2321. We also concur with the Majority members recommendation to add limited-scope COTS exceptions to 10 USC 2320 and 10 USC 2321.

We urge the Secretary of Defense to non-concur on the statutory proposal regarding 10 USC 2320 to always require negotiations regarding additional data rights for COTS items, and on the statutory proposal regarding 10 USC 2321(a) for case-by-case application of the validation scheme, in his recommendations to the congressional defense committees for the following reasons:

- The proposal unduly increases DoD's risk regarding organic sustainment of its weapons systems and future competitive procurements
- The proposal unduly limits DoD implementation of MOSA
- It unduly limits small business participation in defense contracts
- It unduly increases vendor-lock which will exacerbate the excessive pricing that DoD has experienced and will continue to experience for the foreseeable future.
- It does not serve the needs of the warfighter in the dynamic realm in which DoD operates.
- It does not serve the interest of the American taxpayer.

20. How to keep CDRL deliverable up-to-date

Tension Point

An emphasis on ordering data for purposes of maintenance and sustainment must also account for keeping that data current

Issue

The Panel has received Government comments about the need to ensure it receives a complete technical data and software data package for purposes of long term sustainment and maintenance. The Defense Logistics Agency, as well as aftermarket support providers, commented that the lack of data is a factor in sole sourcing such long term sustainment and maintenance to the OEM. While it is clear that a failure to order data and a lack of data rights in delivered data could inhibit long term sustainment and maintenance using third parties or manufacturing spare parts, the Panel also received information from government and industry that the lack of current data is as big a factor as the lack of data itself. In essence, if the Government orders data needed for sustainment, the Government needs to account for that data going stale and needing to be updated to reflect changes in the component.

Discussion

When the Configuration Management changes from contractor to Government, or between Government design and sustaining activities, the IP Strategy should address how to coordinate contractor and Government changes or intra Government entities changes. Further, when the item or software configuration changes, this causes changes in the data and the data rights. The IP Strategy needs to account for how to coordinate Contractor and Government changes for the same item or software.

For every NSN item in a system, there is a Government Primary Inventory Control Activity (PICA) and a Secondary Inventory Control Activity (SICA) identified (DLA, Army, Navy, Air Force, etc.), wherein the contracting and supply management responsibilities are transferred to them for that part/component/assembly. While the configuration management responsibilities might lie with the prime contractor or the Government (acting on behalf of the PM), technical data is transferred to these PICA/SICA agencies so they can manage the inventories of that item, to include the purchasing of additional inventory. Oftentimes, the technical data that the program transfers to these PICA/SICAs is not adequately updated. When the PICA/SICA goes to use the available technical data to competitively or sole source re-procure these items, they find out that the technical data no longer describes the item being used in the manufacture of the system.

One of the Integrated Product Support Elements (IPSE) which are to be addressed in the system Life Cycle Sustainment Plan (LCSP) is supply support and another IPSE is technical data. As the Product Support Manager (PSM) and/or the Product Support Integrated Product Team (PSIPT) plans and executes the LCSP some of the things that should be addressed are the identification of these PICA/SICAs and the transfer of technical data to these PICA/SICAs along with how to update that technical data.

Because the planning, implementation, execution, and oversight of the LCSP involves the identification of technical data and technical data deliverables, there is a direct linkage to the program's IP Strategy. In fact, at Milestone C the IP Strategy is to be part of the LCSP. Therefore, the LCSP and/or the IP Strategy should address how the necessary data will be updated. Potential tools to maintain data currency include priced options, specifically negotiated licenses, escrow or other deferred delivery requirements, reverse engineering, and second sourcing mechanisms.

The Panel notes that there is currently no authoritative document, manual, or instruction which is used to provide uniform instruction to DoD employees to ensure the IP Strategy, LCSP, and DFARS requirements for data planning are coordinated when responsibility for managing a part changes from the acquiring program to another program, such as DLA. This observation is not unique to this topic.

The Panel also notes that an industry standard for commercial items to maintain data currency is through use of subscription agreements. Such agreements are common for data libraries, including for industry standards. Currently, the Panel is not aware of any DFARS direction on how to keep maintenance data current other than to order it from the component OEM or attempt to reverse engineer the latest component configuration to get this new data. However, data subscription agreements may be another tool to maintain data currency.

Recommendation

The Panel does not recommend any changes to 10 U.S.C. 2320 or 2321.

The Panel recommends that changes be made in regulations and/or policy to address the need for a mechanism to maintain currency of the data for the lifetime of the product, including consideration of priced options, specifically negotiated licenses, escrow or other deferred delivery requirements, data subscription agreements, reverse engineering, and second sourcing mechanisms.

The below are recommended changes to the DFARS

227.7103-2 Acquisition of technical data.

(b)(1)

(A) Data managers or other requirements personnel other than pertaining to major weapons systems (or major systems) are responsible for identifying the Government's minimum needs for technical data. Data needs must be established giving consideration to the contractor's economic interests in data pertaining to items, components, or processes that have been developed at private expense; the Government's costs to acquire, maintain, store, retrieve, and protect the data; reprocurement needs; repair, maintenance and overhaul philosophies; spare and repair part considerations; and whether procurement of the items, components, or processes can be accomplished on a form, fit, or function basis. When it is anticipated that the Government will obtain unlimited or government purpose rights in technical data that will be required for competitive spare or repair parts procurements, such data should be identified as deliverable data items. Reprocurement needs may not be a sufficient reason to acquire detailed manufacturing or process data when items or components can be acquired using performance specifications, form, fit and function data, or when there are a sufficient number of alternate sources which can reasonably be expected to provide such items on a performance specification or form, fit, or function basis.

(B) Data managers or other data requirements personnel pertaining to major weapons systems (or major systems) to, in accordance with an IP Strategy (as applicable), identify are responsible for identifying the Government's minimum needs for technical data and the program shall ensure the IP Strategy and the Life Cycle Sustainment Plan (LCSP) incorporates a mechanism to maintain and update the data items. Data needs must be established giving consideration to the contractor's economic interests in data pertaining to items, components, or processes that have been developed at private expense; the Government's costs to acquire, maintain, store, retrieve, and protect the data; reprocurement needs; repair, maintenance and overhaul philosophies; spare and repair part considerations; and whether procurement of the items, components, or processes can be accomplished on a form, fit, or function basis. When it is anticipated that the Government will obtain unlimited or government purpose rights in technical data that will be required for competitive spare or repair parts procurements, such data should be identified as deliverable data items and monitored by the Data Manager, and, in coordination with the Product Support Manager or other product support staff, the program shall ensure the IP Strategy incorporates a mechanism to maintain and update the data items. Data requirements personnel should consider as mechanisms to maintain and update the data items for future needs, such as priced options, specifically negotiated licenses, escrow or other deferred delivery requirements, data subscription agreements, reverse engineering, and second sourcing mechanisms. Reprocurement needs may not be a sufficient reason to acquire detailed manufacturing or process data when items or components can be acquired using performance specifications, form, fit and function data, or when there are a sufficient number of alternate sources which can reasonably be expected to provide such items on a performance specification or form, fit, or function basis.

227.7203-2 Acquisition of noncommercial computer software and computer software documentation.

(b)(1)

(A) Data managers or other requirements personnel other than pertaining to major weapons systems (or major systems) are responsible for identifying the Government's minimum needs. In addition to desired software performance, compatibility, or other technical considerations, needs determinations should consider such factors as multiple site or shared use requirements, whether the Government's software maintenance philosophy will require the right to modify or have third parties modify the software, and any special computer software documentation requirements.

(B) Data managers or other requirements personnel pertaining to major weapons systems (or major systems) to, in accordance with an IP Strategy (as applicable), identify are responsible for identifying the Government's minimum needs, establish a configuration management philosophy with the program and ensure the IP Strategy and the Life Cycle Sustainment Plan (LCSP) incorporates a mechanism to ensure any Government modified software is coordinated with the software provider where the software provider will be providing updates and warranty updates on the software. In addition to desired software

performance, compatibility, or other technical considerations, needs determinations should consider such factors as multiple site or shared use requirements, whether the Government's software maintenance philosophy will require the right to modify or have third parties modify the software, and any special computer software documentation requirements. Where the Government's software maintenance philosophy may include modifications to the software, the Data Manager will need to establish a configuration management approach with the program and, in coordination with the Product Support Manager or other product support staff, ensure the IP Strategy incorporates a mechanism to ensure any Government modified software is coordinated with the software provider where the software provider will be providing updates and warranty updates on the software. Data requirements personnel should consider as mechanisms to maintain and update the software items for future needs tools such as priced options, specifically negotiated licenses, escrow or other deferred delivery requirements, data subscription agreements, reverse engineering, and second sourcing mechanisms.

227.7202-5 Software subscription or software as a service agreements.

A specific contract clause governing the Government's rights in software subscription or software as a service agreements is not prescribed. As required by 227.7202-3, the Government's rights to use, modify, reproduce, release, perform, display, or disclose computer software or computer software documentation obtained under a subscription or service agreement shall be identified in a license agreement.

The below are recommended changes to the DoD Instruction 5000.02 or other appropriate guidance to incorporate consideration of update mechanisms in the IP Strategy using language such as the below:

IP Strategy. Program management must establish and maintain an IP Strategy to identify and manage the full spectrum of IP and related issues (e.g., technical data and computer software deliverables, patented technologies, and appropriate license rights) from the inception of a program and throughout the life cycle. The IP Strategy will describe, at a minimum, how program management will assess program needs for, and acquire competitively whenever possible, the IP deliverables and associated license rights necessary for competitive and affordable acquisition and sustainment over the entire product life cycle, including by integrating, for all systems, the IP planning elements required by subpart 207.106 (S-70) of the Defense Federal Acquisition Regulation Supplement (Reference (a1)) for major weapon systems and subsystems thereof. The IP Strategy will be updated throughout the entire product life cycle, initially as part of the Acquisition Strategy, and during the Operations and Support Phase as part of the Life-Cycle Sustainment Plan.

The IP Strategy will designate a specific point of contact in the program who will be responsible for maintaining and implementing the IP Strategy. The IP Strategy will have risk assessments that correspond to changes in sustainment philosophies, and changes in configuration management, changes in the item or software configuration. Further, when the Configuration Management for a Contractor item changes from Contractor to Government, the IP Strategy needs to account for coordination Contractor changes to the Government item and Government changes to the Contractor item. The IP Strategy will further document an acquisition strategy and be aligned with the LCSP regarding data/data rights for each component, which will be maintained at a depot performed solely by Government personnel, which components will be supported by a contractor either directly or under the direction of

the depot, when such depot maintenance will begin, the method by which received data items are maintained and kept up to date as the component is updated, and whether transition assistance is needed presently or in the future should the component OEM no longer support the component. The IP Strategy should consider, as tools, priced options, specifically negotiated licenses, escrow or other deferred delivery requirements, data subscription agreements, reverse engineering, and second sourcing mechanisms.

The Panel recommends the Secretary create an authoritative document, manual, or instruction which is used to provide uniform instruction to Department employees to coordinate the execution of the IP Strategy, LCSP, and DFARS requirements for data planning.

The Panel also recommends that training be available to Government and industry to increase awareness of the need to maintain data currency during the program lifecycle.

21. Small Business Innovation Research (SBIR) (Flow-down to Suppliers; Inability to Share with Primes; Evaluation)

Tension Point

SBIR Mandatory Data Rights provisions for Phase III (non-SBIR funded) Contracts or Subcontracts

Issue

10 U.S.C. 2320 states that the establishment of any rights in technical data should include consideration of the Small Business Innovation Development Act of 1982 (15 U.S.C. 638 note), and the Small Business Act (15 U.S.C. 631). This legislation established the SBIR program with the purpose of strengthening the role of small, innovative firms in federally funded research and development. Small business DoD contractors are rewarded for their innovation and invention in the SBIR program by receiving a special class of SBIR technical data rights, delineated for DoD contracts in DFARS 252.227-7018¹. SBIR technical data rights apply to all SBIR awards, including subcontracts to such awards, that fall within the statutory definition of Phase I, II, or III of the SBIR Program.

Discussion

15 U.S.C. 638(e)(4)(C) states that a Phase III award is one that: *derives from, extends, or completes efforts made under prior funding agreements under the SBIR program—*

- (i) *in which commercial applications of SBIR-funded research or research and development are funded by non-Federal sources of capital or, for products or services intended for use by the Federal Government, by follow-on non-SBIR Federal funding awards; or*
- (ii) *for which awards from non-SBIR Federal funding sources are used for the continuation of research or research and development that has been competitively selected using peer review or merit-based selection procedures.*

Phase III work is typically oriented towards commercialization of SBIR research or technology and may be either a competitive or non-competitive award of a contract, or a subcontract, to a small business. SBIR data rights clauses are non-negotiable and must not be the subject of negotiations pertaining to a SBIR Phase III award, or diminished or removed during award

¹ <https://www.gpo.gov/fdsys/pkg/CFR-2009-title48-vol3/pdf/CFR-2009-title48-vol3-sec252-227-7018.pdf>

administration². During Panel deliberations and comments provided by small businesses to the Panel, the following tension points were raised which related to follow-on “Phase III” awards where SBIR data rights clauses would apply.

By law, an agency must not, in any way, make issuance of a SBIR Phase III award conditional on relinquishing data rights. Moreover, in the FY 2012 NDAA, special acquisition preference was clarified for SBIR/STTR and goals were set for SBIR-STTR Technology Insertion. As a result, USD (AT&L) Memo “Implementation Directive for Better Buying Power 2.0 (24 APR 2013)” and DoDI 5000.02 issued direction for program managers with contracts with a value at or above \$100 million to establish goals for the transition of Phase III technologies in subcontracting plans and require primes to report the number and dollar amount of Phase III SBIR or STTR contracts. The Panel heard that based on direction from ASN (RDA) the Navy now requires PEO-level formulation of a Small Business strategy with DPM support as “... the Small Business Advocate responsible for identifying opportunities within the program for Small Business participation.” The DON Phase III Guidebook includes examples of SBIR/STTR incentives that COs and/or CORs may use in supporting PMs, PEOs, and CAEs in responding to these requirements, and includes candidate language for inclusion in Sections C, I, L, and M of an RFP. This type of specific guidance is not yet included though in the broader agency-wide Defense Acquisition Guidebook.

When prime contractors elect to make a subcontract award to a small business supplier if the award would *“derive from, extend, or complete efforts made under prior funding agreements under the SBIR program”* then the subcontract would be considered a Phase III award and the law requires that the SBIR data rights clause (DFARS 252.227-7018) must be included in the subcontract. This creates an issue if there is a mandatory flow-down of Government Purpose Rights (GPR) data rights from the prime contractor (see Tension Point 19) as SBIR data rights are non-negotiable, even if the prime contract includes non-SBIR data rights clauses (DFARS 252.227-7013³ and 252.227-7014⁴).

The panel discussed SBIR Phase III issues that can arise, when data rights are used as an evaluation factor (see Tension Point 4) or when unlimited data rights or GPR are required as a condition of award (see Tension Point 1). If a prime contractor’s response includes subcontracted work to a small business that “derives from, extends, or completes efforts made under prior funding agreements under the SBIR program” then that work would be considered a SBIR Phase III. By law, SBIR data rights accord to any contract that would be considered a SBIR Phase III, even if the solicitation provides for other rights, and an agency must not, in any way, make issuance of a SBIR Phase III award conditional on data rights. If a prime contractor

² <https://www.sbir.gov/about/about-sbir#sbir-policy-directive>

³ <https://www.gpo.gov/fdsys/pkg/CFR-2011-title48-vol3/pdf/CFR-2011-title48-vol3-sec252-227-7013.pdf>

⁴ <https://www.gpo.gov/fdsys/pkg/CFR-2011-title48-vol3/pdf/CFR-2011-title48-vol3-sec252-227-7014.pdf>

proposes use of a SBIR developer as a subcontractor, the law would prohibit inclusion of SBIR data rights as a factor in the evaluation of the prime contractor.

Similarly, small businesses pointed to issues when a competitive solicitation, such as a BAA, required delivery with unlimited data rights (e.g. DFARS 252.227-7013). If the proposed approach would be considered a Phase III effort, then the law requires that issuance of a contract could not be conditioned on relinquishing SBIR data rights. If the SBIR awardee wishes to transfer its SBIR data rights to the awarding agency or to a third party, it must do so in writing under a separate agreement. A decision by the awardee to relinquish, transfer, or modify in any way its SBIR data rights must be made without pressure or coercion by the agency or any other party and any other data rights agreement must be entered into only after the SBIR Phase III award, which includes the appropriate SBIR data rights clause, has been signed.

While SBIR technical data rights allow the Government to use technical data for Government purposes, to protect the competitive interests of the small business, there are restrictions on the disclosure of this data outside of the Government, including disclosure for procurement purposes (FAR 52.227-20). A tension point was raised that this restriction made it difficult for the Government to share technical SBIR data with their primes for evaluation of whether the innovations developed by the small business could be leveraged within a program of record. During the SBIR data rights protection period, the SBIR Policy Directive § 8(b)(2) requires agencies protect from disclosure and nongovernmental use all SBIR technical data developed from work performed under an SBIR funding agreement unless, subject to paragraph (b)(3), the agency obtains permission to disclose such SBIR technical data from the awardee or SBIR applicant. DFARS 252.227-7018 provides five years of data rights protection for SBIR/STTR data from the date of the last contract deliverable. This data rights protection period will be extended if the SBIR/STTR data is protected and referenced under a subsequent SBIR/STTR contract. The Panel heard that this problem is currently handled by primes establishing an NDA directly with the small business in order to receive technical data protected by SBIR data rights.

The Panel discussed recommendations on how to consider data rights solutions in relation to program needs, in particular for life cycle support (see tension points 10, 11 and 12). The Department of the Navy SBIR and STTR Phase III Guidebook⁵, presents methods on how SBIR/STTR technology can be used to realize mission cost savings and technology objectives, and recommends approaches for SBIR/STTR inclusion in program planning and management over program life cycles. These included guidance on how to handle flow-down of the SBIR/STTR data rights clauses in a subcontract from a prime, how to introduce competition by working with the small business to develop a second source for SBIR developed technology, and how to handle award to another company, in accordance with the SBA Policy Directives, in the event of poor performance by a SBIR company.

⁵http://www.secnav.navy.mil/smallbusiness/Documents/DON%20SBIR_STTR%20Guidebook_09.16.2014%20final.pdf

The Panel also discussed how to handle SBIR data rights with respect to major system interfaces. The FY2017 NDAA provides for GPR in technical data pertaining to major systems interfaces (MSI) that is (i) developed either exclusively at private expense or with mixed funding and (ii) used in a modular open system approach (MOSA), under the condition that the Secretary of Defense shall negotiate with the contractor the appropriate and reasonable compensation for such technical data (see Tension Point 29 and 10 U.S.C. 2320(a)(2)(G)). While the Government is prohibited from making an award conditional on relinquishing SBIR data rights, the SBA Policy Directives² do allow, after an award is made, for the Government to negotiate with the contractor the appropriate and reasonable compensation for acquiring GPR for SBIR data rights protected technical data. The panel has made recommendations on statutory changes to clarify handling of SBIR protected data in MSI.

Industry panelists expressed a concern about applying the doctrine of segregability to SBIR data in regulatory implementation. In situations where a small business' item or process will be incorporated into or merged with an item or process developed at least in part with Government funds, the Government would obtain GPR to the resulting technical data or software deliverables unless the parties segregate the SBIR data or software from the data or software pertaining to the portions of the item or process developed at least in part with Government funds. In such situations, the onus will be on the small business to take the steps necessary to protect segregable portions of the SBIR data/software. Additional training would be helpful to educate small businesses about the risks associated with integrating SBIR technology into items or processes otherwise developed at least in part with Government funding.

The panel also discussed the lack of appeal rights for small businesses asserting SBIR data rights as a subcontractor as, under the Contractor Disputes Act (CDA), only a contractor may appeal to the Armed Services Board of Contract Appeals (ASBCA) (see Tension point 18)⁶.

Recommendation

The Panel recommends the following statutory revisions to 10 U.S.C. 2320(a)(2)(A) to clarify that for the purpose of 10 U.S.C. 2320, an item or process developed under a contract or subcontract to which the SBIR regulations apply shall be treated as though developed at private expense during the protection period authorized in the SBIR regulations:

"(A) Development exclusively with Federal funds. (i) Except as provided in subparagraph (ii), in the case of an item or process that is developed by a contractor or subcontractor exclusively with Federal funds, the United States shall have the unlimited right to--

⁶Binghamton Simulator Company (BSC) ASBCA decision 59117

"(I) use technical data pertaining to the item or process; or

"(II) release or disclose the technical data to persons outside the Government or permit the use of the technical data by such persons.

"(ii) Small business innovation research. An item or process developed under a contract or subcontract to which regulations under section 9(j)(2) of the Small Business Act (*15 U.S.C. 638(j)(2)*) apply shall be treated as an item or process developed at private expense, except as otherwise permitted by those regulations. Upon the expiration of the protection period authorized in those regulations, the rights of the United States shall be as set forth in subparagraph (i). "

The panel also recommends the following regulatory changes:

- Amend DFARS to clarify that a change in data rights clause can be flowed down based on whether the subcontractor or supplier is eligible for SBIR protections:

DFARS 252.227-7013

...

(k) Applicability to subcontractors or suppliers. (1) The Contractor shall ensure that the rights afforded its subcontractors and suppliers under 10 U.S.C. 2320, 10 U.S.C. 2321, and 15 U.S.C. 638, and the identification, assertion, and delivery processes of paragraph (e) of this clause are recognized and protected.

...

(6) The Contractor shall include the substance of the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovation Research (SBIR) Program clause set forth at 252.227-7018 of the Defense Federal Acquisition Regulation Supplement (DFARS), in all subcontracts for technology within the scope of the SBIR program, as defined in DFARS 227.7104, and for which the subcontractor has asserted SBIR data rights

Make Like changes to DFARS 252.227-7014 and 252.227-7015

DFARS 252.227-7018

(k) Applicability to subcontractors or suppliers. (1) the Contractor shall assure that the rights afforded its subcontractors and suppliers under 10 U.S.C. 2320, 10 U.S.C. 2321, and 15 U.S.C. 638, and the identification, assertion, and delivery processes required by paragraph (e) of this clause are recognized and protected.

...

(6) Whenever any noncommercial technical data or computer software which is not restricted under the SBIR program and is to be obtained from a

subcontractor or supplier who is not in the SBIR program, for delivery to the Government under this contract, the Contractor shall use the Rights in Technical Data—Noncommercial items clause set forth in 252.227-7013 of the Defense Federal Acquisition Regulation Supplement (DFARS) for non-commercial technical data, or the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause set forth in 252.227-7014 of the DFARS in the subcontract or other contractual instrument, and require its subcontractors or suppliers to do so, without alteration, except to identify the parties. The Contractor shall use the Technical Data—Commercial Items clause set forth in 252.227-7015 of the DFARS to obtain technical data pertaining to commercial items, components, or processes. No other clause shall be used to enlarge or diminish the Government's, the Contractor's, or a higher tier subcontractor's or supplier's rights in a subcontractor's or supplier's technical data or computer software.

- The Panel recommends that the assertion tables in DFARS 252.227-7017, 252.227-7013, and 252.227-7014 have a basis for assertion which directly references SBIR data rights protection in addition to those bases for assertions related to funding. (See DFARS case 2010-D001)
- The panel recommends an update in Defense Acquisition Guidebook at <https://dag.dau.mil/> and Department of Defense Source Selection Procedures to provide specific guidance for inclusion of SBIR/STTR technologies in acquisition programs, similar to the guidance provided by the Navy in their DON Phase III Guidebook⁵.
- SBIR

The panel recommends that additional training would be helpful to educate small businesses about the risks associated with integrating SBIR technology into items or processes otherwise developed at least in part with Government funding.

22. Lack of Trained Personnel

Tension Point

Generally, Government program managers (PMs), engineers, contracting officers (COs), requirements and logistics officers - do not possess sufficient knowledge and skills regarding the management of Technical Data and Computer Software Rights.

Issue

Acquisition professionals do not receive adequate, if any, training in this area, therefore, they may not be able to define government needs for life cycle sustainment when their leverage is most practical – in the early phases of a program. As a result, they request Unlimited or Government Purpose Rights, even when the acquisition program may not require this level of rights in technical data or computer software.

Discussion

Policy - It is DoD policy (DFARS 227.7103-1) to acquire only the technical data, and the rights to that data, necessary to satisfy agency needs. Solicitations and contracts must (1) Specify the technical data to be delivered under a contract and the delivery schedules for the data; (2) Establish or reference procedures for determining the acceptability of technical data; (3) Establish separate contract line items, to the extent practicable, for the technical data to be delivered and require offerors and contractors to price separately each deliverable data item; and (4) Require offerors to identify, to the extent practicable, technical data to be furnished with restrictions on the Government's rights and require contractors to identify technical data to be delivered with such restrictions prior to delivery.

Reality - Anecdotal evidence as well as reports from the Government Accountability Office (GAO) indicate that DoD has not always developed a viable Intellectual Property strategy for its acquisitions. Furthermore, government requirements for technical data and software may not be precisely defined by acquisition personnel assigned to execute the program. This is due partly to the dynamic, uncertain nature of the defense realm and partly to the acquisition personnel's inability to "predict" the future and determine exactly what technical data will be needed several years into the life cycle. (What exactly will we need five, ten or more years into the future to sustain the program and when exactly will we need it?) In addition to the difficulty of accurately estimating future technical data requirements, acquisition personnel across most "Acquisition" disciplines lack basic training and an in depth understanding of technical data and computer software acquisition. Thus, acquisition personnel opt to acquire as much data and software as they can, in the early phase of the program – prior to contract award - while DoD still has considerable leverage and insight into its investment - even if all the data will not be needed until later in the sustainment phase of the program or at any time in the future.

Despite policies to the contrary, this practice has been encouraged by the hard-learned lessons these personnel have gathered in defense acquisition. What experience has taught them, and again what has been confirmed in GAO reports, is that when DoD personnel do not acquire as much data and software as they can in the early phases of the program, they face major obstacles in obtaining, at a reasonable cost, the data rights necessary to sustain the system.

Summary -

1. Requirements owners/generators do not, typically, possess sufficient knowledge to accurately assess future government requirements therefore the default position is to request “everything”.
 - a. The dynamic, uncertain realm in which DoD operates complicates this further.
 - b. It is difficult for DoD to assess its future data and software needs in the early phase of the program but the market forces compound the problem if DoD defers the decision for data until the later phases of the program.
 - c. It is not clear whether DOD can acquire data and software in the later phases of the program and, when it does, what a reasonable price would be to pay, particularly when large sums have been expended in development.
2. At times, COs may not negotiate the appropriate data rights into their contracts, or do not address them appropriately because the requiring activity has not requested the data or has not provided sufficient supporting information.
3. Even when COs include data rights requirements in the contract, data requirements may be unclear. They may not be addressed in the CDRLs but even when data rights are adequately addressed, DoD may not receive delivery of the data. DoD should ensure the contract includes the requirement for delivery of the data it needs.

Recommendation

To ameliorate the situation, we recommend a two-prong approach to be addressed in legislation **(1) Require/Provide additional training for acquisition personnel and (2) Develop a Cadre of Subject Matter Experts.**

- 1. Require/Provide mandatory training for acquisition personnel assigned to specific programs**
 - a. To raise the awareness level and enhance knowledge, ensure all program managers (PMs), engineers, requirements owners (ROs), contracting officers (COs) and logistics officers receive “Just-in-Time” specialized training on technical data and computer software acquisition, prior to assigning them responsibilities in acquisitions which require technical data and software rights.
 - b. Make technical data and software rights one of the “core” subjects required prior to certification of Level III PMs, and COs and Core Plus - Life Cycle Logistics.
 - c. Streamline and simplify data and software acquisition practices so they will be easier to implement effectively.

2. Develop a Cadre of Subject Matter Experts (SMEs)

- a. The cadre should consist of SMEs from the world of requirements generators - those who understand the requirements and potential future needs, from contracting, logistics and legal.
- b. Similarly to Peer Reviews, the individuals selected for this assignment should be fairly senior individuals, with broad-based knowledge of their particular field. They should possess considerable experience across “Acquisition”, and should have completed training and obtained experience in the management of data rights.
- c. This assignment need not be a full-time duty. Initially, it can be handled as an additional duty in the same manner we handle the DoD Peer Reviews and the Air Force Multifunctional Independent Review Teams (MIRTS).
- d. Although these experts may be assigned to their respective agencies, the tasking to help formulate and review Intellectual Property strategy of major systems and appropriate services acquisitions should come from a centralized location at the Office of the Secretary of Defense, e.g. DPAP. This scheme will enable a smaller cadre of individuals to cover a greater number of programs and will eventually standardize, to the degree possible, the DoD requirements for technical data rights and software for our weapons systems and related services.
- e. This cadre should also be tasked with recommending how data and software acquisition practices should be streamlined and simplified to ease training and implementation burdens.

Neither of these recommendations are a panacea but jointly they could go a long way in improving the present situation.

NOTE: Recommendation # 2 – “Develop a Cadre of Subject Matter Experts (SMEs)” was adopted by the U.S. House Armed Services Committee (HASC) immediately upon publication of this paper. It was included in the Fiscal Year 2018 National Defense Authorization Act.

Attachment: Proposed Legislation

SEC. XXXXX MANDATORY REQUIREMENT FOR TRAINING RELATED TO TECHNICAL DATA AND COMPUTER SOFTWARE RIGHTS AND INTELLECTUAL PROPERTY

(a) MANDATORY TRAINING FOR TECHNICAL DATA AND COMPUTER SOFTWARE RIGHTS - Section xxxx of title XX, United States Code, is amended by adding the following new subsection:

(xx) TECHNICAL DATA AND COMPUTER SOFTWARE RIGHTS AND INTELLECTUAL PROPERTY TRAINING REQUIRED - The Secretary of Defense shall provide mandatory training for members of the Defense Acquisition workforce and employees of the Department of Defense responsible for the acquisition of defense articles and commercial items.

(xx). Such mandatory training shall, at a minimum, provide comprehensive guidance, methodologies and best practices for:

- (1) the subject, the function and the impact of technical data and computer software rights and intellectual property in the acquisition of defense articles and commercial items;
- (2) recognizing the need to address technical data and computer software rights prior to issuance of the requirements documents and prior to the issuance of the Request for Proposals;
- (3) more accurate estimating needs for data rights for the sustainment phase of a program;
- (4) specifically negotiated license rights as an alternative to standard license rights;
- (5) development of Intellectual Property Strategies

(b) INCORPORATION INTO DEFENSE ACQUISITION WORKFORCE LEVEL III CERTIFICATION

- (1) Members of the Defense Acquisition Workforce and other employees of the Department of Defense must receive the appropriate training prior to an assignment to an acquisition coded position and before they are certified Level III.
- (2) Department of Defense Office of General Counsel shall consider the feasibility of establishing equivalent training and certification for acquisition and intellectual property attorneys.

SEC. XXX REQUIREMENT TO ESTABLISH A CADRE OF SUBJECT MATTER EXPERTS REGARDING TECHNICAL DATA AND COMPUTER SOFTWARE RIGHTS AND INTELLECTUAL PROPERTY

- (a) ESTABLISHMENT OF CADRE OF SMEs IN TECHNICAL DATA AND COMPUTER SOFTWARE RIGHTS - The Secretary of Defense shall establish a cadre of Subject Matter Experts (SMEs) within the Department of Defense who will provide advice and expertise in the planning and estimating of requirements regarding technical data and computer software rights for defense acquisitions of defense articles and commercial items.

(xx) This cadre will be established within one calendar year from the effective date of this authorization.

- (b) REPORT TO CONGRESS

Upon implementation of the above requirement, and no later than a year from the date of this authorization, the Secretary of Defense shall provide a report to Congress notifying them of the establishment of the cadre of SMEs.

23. The Data Assertion List is a Burden on both Contractors and Government

Tension Point

The existing Data Assertion List is a burden for both contractors to prepare and Government to receive and may result in contract performance delays. The form has remained the same since 1995, but Government needs for the Data Assertion List have changed.

Issue

The Panel has received industry comments that there has been an increased burden with complying with the data assertions list. Specifically, there is confusion between the data assertion list creation and update processes in DFARS 252.227-7017, DFARS 252.227-7013 and 252.227-7014, and the challenge process for delivered data in DFARS 252.227-7037 and 252.227-7019.

Discussion

The contractor's ability to add new assertions to an assertion list under DFARS 252.227-7013 and 252.227-7014 is governed by a separate process which does not affect the Government's ability to challenge the data on delivery. Such challenges to adding new assertions has led to contract delays if CDRLs are not accepted due to this misunderstanding, and proposal delays as contracting officers attempt to validate the assertion lists prior to awarding the contract.

The Panel received industry comments that the Government is increasing the burden of completing the existing Data Assertion List through H clauses requiring listing of commercial data or by requiring each listed assertion correlate with a CDRL, or statement of work requirements, or CLIN requirements. The Panel received a similar comment from Government presenters, who indicate that the existing listing is not useful and should correlate more closely to how the Government tracks development activities (such as to WBS codes) for technologies. Such an approach may also be more aligned with the IP Strategy required under DoD Instruction 5000.02. Government comments also indicate such a structure might be useful in tying color codes to source of developmental funds determinations for spare parts or components for work performed under the contract (or multiple contracts). As such, the existing table format may not be meeting the current government needs, and may need to be updated.

In regards to commercial data, the Panel received comments that the existing form used in DFARS 252.227-7017 does not accommodate commercial items, and that the forms required in DFARS 252.227-7017, 252.227-7013 and 227.227-7014 are not appropriate for commercial data or to be flowed to commercial suppliers. The comment indicated that prior identification of commercial restrictions needs to be in accordance with commercial terms and conditions, and should identify such restrictions according to definitions in FAR 2.101. There is no mechanism for commercial data (especially software or firmware) which are not licensed since the author relies on copyright restrictions in 17 U.S.C.

The Panel also received industry comments that, while DFARS 252.227-7017 is clear that the initial data assertion list is added as a contract attachment, it is not clear whether the updates to the assertion lists under DFARS 252.227-7013(e) and 252.227-7014(e) are effective as of the date of receipt or if the updates must be added as an update to the contract attachment. Since Contract Data Requirement Lists (CDRLs) cannot be delivered until these updates are effective, the uncertainty on when the updates are effective can lead to contractual delays. Further, the two clauses create duplicate reporting requirements for technical data updates (DFARS 252.227-7013(e)) versus software (DFARS 252.227-7014(e)). Further, by including these requirements in DFARS 252.227-7013 and 252.227-7014, this requires these update requirements be a flowdown to suppliers which is in contrast to DFARS 252.227-7017, which is created by the prime using data from the suppliers.

The Panel also received a suggestion to possibly combine two clauses: DFARS 252.227-7017 and 252.227-7028. DFARS 252.227-7028 is a separate data assertion list which can be used to identify data which was delivered under a different contract. Since contractors commonly deliver the same technical data on multiple contracts, this clause would allow the contractor to rely on an existing data assertion list for submission. DFARS 252.227-7028 is underutilized and would simplify some of the disputes caused by identification of data under DFARS 252.227-7017. The suggestion would be to eliminate DFARS 252.227-7028, and add a column to DFARS 252.227-7017 to identify the contract under which the data was delivered. This combination would prevent rework for both Government and industry where data is already in the Government inventory.

The Department had previously suggested in DFARS Case 2010-D001 & DFARS Case 2013-D028 which are consistent with these observations.

Recommendation

The Panel does not recommend any changes to 10 U.S.C. 2320 or 2321.

The Panel does recommend changes be made to the DFARS

227.7102-2 Rights in technical data.

(c) An identification prior to delivery of any commercial technical data to be delivered to the Government with restrictions on use shall be in accordance with commercial terms and conditions, and need not be required in all proposals. Where required, such identification can be done by a higher tier supplier or the Contractor on behalf of the owner of the commercial technical data under DFARS 252.227-7017 or 252.227-70XX.

227.7202-3 Rights in commercial computer software or commercial computer software documentation.

(c) An identification prior to delivery of any commercial software or commercial computer software documentation to be delivered to the Government with restrictions on use shall be in accordance with commercial terms and conditions, and need not be required in all proposals. Where required, such identification can be done by a higher tier supplier or the Contractor on behalf of the owner of the commercial technical data under DFARS 252.227-7017 or 252.227-70XX.

DFARS 227.7202 should further be updated to recognize copyright restrictions under 17 U.S.C. for copyrighted commercial works which are not licensed, such as firmware or embedded software.

Delete DFARS 252.227-7013(e) and 252.227-7014(e) and create new combined clause for post award assertion list updates:

DFARS 252.227-70XX Post Award Identification and assertion of use, release, or disclosure restrictions.

(a) Except as provided in paragraph (b) of this clause, technical data or computer software that the Contractor asserts should be furnished to the Government with restrictions on use, release, or disclosure are identified in an attachment to this contract (the Attachment). The Contractor shall not deliver any data with restrictive markings unless the data are listed on the Attachment.

(b) In addition to the assertions made in the Attachment, other assertions may be identified after award when based on new information or inadvertent omissions unless the inadvertent omissions would have materially affected the source selection decision. Such identification and assertion shall be submitted to the Contracting Officer as soon as practicable prior to the scheduled date for delivery of the data, in the following format, and signed by an official authorized to contractually obligate the Contractor:

Post Award Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Technical Data or Computer Software.

The Contractor asserts for itself, or the persons identified below that the Government's rights to use, release, or disclose the following technical data or computer software should be restricted

Technical Data or Computer Software to be Furnished With Restrictions*	Basis for Assertion**	Asserted Rights Category***	Name of Person Asserting Restrictions****	Contract number where previously delivered (if any)
(LIST)	(LIST)	(LIST)	(LIST)	(LIST)

*For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such items, component, or process. For computer software or computer software documentation identify the software or documentation.

**Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions for non-commercial data. For commercial data, the basis for assertion is whether the item or software is a commercial item or process. For SBIR data, the data was generated under the SBIR program. For non-commercial technical data, other than computer software documentation, development refers to development of the item, component, or process to which the data pertain. The Government's rights in non-commercial computer software documentation generally may not be restricted. For non-commercial computer software, development refers to the software. Indicate whether development was accomplished exclusively or partially at private expense. If development was not accomplished at private expense, or for computer software documentation, enter the specific basis for asserting restrictions.

***Enter asserted rights category (e.g., government purpose license rights, rights in SBIR data, limited, restricted, commercial, government purpose rights, or specially negotiated licenses).

****Corporation, individual, or other person, as appropriate.

Date _____

Printed Name and Title _____

Signature _____

(End of identification and assertion)

(c) Even after the scheduled date for delivery of the data, when requested by the Contracting Officer, the Contractor shall provide sufficient information to enable the Contracting Officer to understand what is being asserted and to ensure the assertion is formatted correctly. Once understood, the Contracting Officer will add the Contractor's assertions to the Attachment if the conditions of (b) are otherwise satisfied, but may do so after the scheduled date for delivery of the data.

(d) The Contracting Officer reserves the right to validate any listed assertion, at a later date, in accordance with the procedures of the Validation of Restrictive Markings on Technical Data or Validation of asserted restrictions—Computer software clause of this contract.

DFARS 252.227-7017 Identification and assertion of use, release, or disclosure restrictions.

(d) The Offeror's assertions, including the assertions of its subcontractors or suppliers or potential subcontractors or suppliers shall be submitted as an attachment to its offer in the following format, dated and signed by an official authorized to contractually obligate the Offeror:

Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Technical Data or Computer Software

The Offeror asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following technical data or computer software should be restricted:

Technical Data or Computer Software to be Furnished With Restrictions*	Basis for Assertion**	Asserted Rights Category***	Name of Person Asserting Restrictions****	Contract number where previously delivered (if any)
(LIST)*****	(LIST)	(LIST)	(LIST)	(LIST)

....

**Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions for non-commercial data. For commercial data, the basis for assertion is whether the item or software is a commercial item or process. For SBIR data, the data was generated under the SBIR program. For non-commercial technical data, other than computer

software documentation, development refers to development of the item, component, or process to which the data pertain. The Government's rights in non-commercial computer software documentation generally may not be restricted. For non-commercial computer software, development refers to the software. Indicate whether development was accomplished exclusively or partially at private expense. If development was not accomplished at private expense, or for computer software documentation, enter the specific basis for asserting restrictions.

***Enter asserted rights category (e.g., government purpose ~~license~~ rights ~~from a prior contract~~, rights in SBIR data ~~generated under another contract~~, limited, restricted, commercial, ~~government purpose rights under this or a prior contract~~, or specially negotiated licenses).

252.227-7028 Reserved Technical data or computer software previously delivered to the government.

24 Deferred ordering period: 6 years (rather than perpetual) and Deferred Ordering Part 1: only data “generated” under the contract (Majority Position)

Tension Point

Recent legislation (and proposed legislation) mandating deferred ordering has substantially increased risks for contractors

Issue

DFARS 227.7103-8(b) prescribes using the Deferred Ordering clause (252.227-7027) when a firm requirement for a particular data item(s) has not been established prior to contract award but there is a potential need for the data. Under the clause, the contracting officer may order any data that has been generated in the performance of the contract or any subcontract thereunder at any time until three years after acceptance of all items (other than technical data or computer software) under the contract or contract termination, whichever is later.

FY2012 NDAA added¹ the following to the list of contract provisions required “whenever practicable” under 10 USC 2320(b):

(9) ... in addition to technical data that is already subject to a contract delivery requirement, the United States 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, upon a determination that—

- (A) the technical data is needed for the purpose of reprocurement, sustainment, modification, or upgrade (including through competitive means) of a major system or subsystem thereof, a weapon system or subsystem thereof, or any noncommercial item or process; and*
- (B) the technical data—*
 - (i) pertains to an item or process developed in whole or in part with Federal funds; or*
 - (ii) 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.... .*

¹ Section 815(a)(2)(C)

Thus, relative to the Deferred Ordering clause that has been used only when firm data requirements have not been established, the foregoing statutory mandate expanded the deferred ordering concept to apply to certain data utilized (as opposed to generated) in the performance of a contract and removed the three-year time limit. Both changes were criticized by industry since they undermined contractual certainty as to the bounds of a particular contract, and also since the unlimited ordering period created uncertainty over whether the contractor had any obligation to keep data used in a particular contract once that data was superseded or otherwise would normally be purged in the normal course of business.²

While the foregoing has yet to be implemented in the DFARS, FY2017 NDAA³ restored the limit of the clause's reach to data generated in the performance of a contract and restoring a time limit (albeit expanded to six years). These changes are critically important and address many industry concerns about the original law, and especially as proposed to be implemented under DFARS Case 2012-D022.

The potential to have to deliver data that has been merely “utilized” in the performance of a contract (even if the technical data, and the technology to which the data pertain, were developed exclusively at contractors’ private expense), at any time, creates uncertainty and IP risk that defies quantification. A likely result would have been a reduction in willingness either to make certain technologies available to DoD or to utilize privately-funded manufacturing processes and tools in the performance of DoD contracts, thereby raising overall procurement costs.

FY2017 NDAA also replaced⁴ the “segregation/reintegration” data requisite⁵ with a reference to certain types of interface data, all of which are either subject to government purpose rights or, if subject to limited rights, subject to authorized release for segregation/reintegration purposes.⁶ It retained the alternative mixed funding requisite.⁷

While the changes were positive, the FY2017 NDAA is likely going to be interpreted as mandating deferred ordering, which is likely to further discourage contractors from adapting sensitive technologies for government needs and also provide a disincentive for government negotiations for data which it believes it will obtain by right under the implementing clause. Under the current regulations, contractors can mitigate their IP risk by carefully defining with the

² CODSIA comment on Defense Federal Acquisition Regulation Supplement: Rights in Technical Data and Validation of Proprietary Data Restrictions (DFARS Case 2012–D022) dated September 30, 2016; Small Business Technology Council’s Comment on Defense Federal Acquisition Regulations Supplement (DFARS) relating to Rights in Technical Data and referenced under Docket DARS-2016-0017/DFARS Case 2012-D022 of September 29, 2016; American Bar Association Section of Public Contract Law comment on DFARS Case 2012-D022, Defense Federal Acquisition Regulation Supplement: Rights in Technical Data and Validation of Proprietary Data Restrictions, 81 Fed. Reg. 39482 (June 16, 2016) dated September 20, 2016.

³ Section 809(c)(1) and (2).

⁴ Section 809(c)(3).

⁵ 10 USC 2320(b)(9)(B)(ii)

⁶ 10 USC 2320 (a)(2), subparagraphs (D)(i)(II), (F), and (G)

⁷ 10 USC 2320(b)(9)(B)(i)

contracting officer what data will be delivered, and contracting officers are required under 10 U.S.C. 2320(b)(2), (3), and (5) to identify the data being provided under the contract in advance. Thus, under the existing process, contracting officers have the flexibility to agree to omit deferred ordering from a contract or to exempt certain data from deferred ordering where the parties clearly understand the scope of the data being generated under the contract so that there is no need to maintain the threat of future data (or software) delivery demands, which threat otherwise would make a contractor unwilling to adapt its sensitive technologies for government needs.

This tension often arises when a contractor or sub-contractor wants to propose modifying a pre-existing, privately funded technology to meet the requirements of an RFP that carries a deferred ordering clause. Depending on the relative markets for the pre-existing and as-to-be-modified technologies, undertaking the modifications may put at-risk commercial profits that are significantly higher than what is expected on the government program. In such a case, the sub-contractor's only commercially viable alternatives may be either not to bid, to propose modifying another (less optimal) technology, or to propose a (more expensive) clean sheet design.

Similarly, mandating deferred ordering in cases of mixed funded developments is likely to further discourage contractors from investing private funds in the development of items or processes. This would be especially problematic for developments for which contractors are asked to shoulder a large portion (sometimes the vast majority) of the development costs or for cases in which the U.S. Government is the primary or exclusive end user of the item or process in question. In such cases, a contractor's willingness to invest is tied to its ability to mitigate its IP risk by carefully defining with the contracting officer what data will be delivered. If a deferred ordering right would attach to any data pertaining to an item or process developed with mixed funding, contractors may reconsider the extent to which they are willing to invest private funds in such developments or make such technologies available to the DoD.

Minority Report: Five members of the panel have submitted a minority report for this tension point, dissenting from the statutory changes recommended by the panel. The majority notes that nothing herein prevents DoD from implementing deferred ordering where it deems appropriate, rather it simply provides DoD with the flexibility to except data from the reach of the mandatory deferred ordering where it deems appropriate. The majority believes the minority's position unnecessarily restricts the DoD's and contacting officers' flexibility in this regard, with the consequences discussed herein.

Recommendation

Amend 10 USC 2320(b)(9) as follows:

(9) ... in addition to technical data that is already subject to a contract delivery requirement, and except for data (other than data described at paragraphs (A) and (G) of subsection (a)(2)) that

the government and the contractor have agreed will not be subject to deferred ordering, the United States may require until the date occurring six years after acceptance of the last item (other than technical data) under a contract or the date of contract termination, whichever is later, the delivery of technical data that has been generated in the performance of the contract, and compensate the contractor only for reasonable costs incurred for having converted and delivered the data in the required form, upon a determination that

The panel discussed the following recommendations regarding items that should be added to the implementing regulations, in order to encourage use of commercial and privately-funded technologies and to create competition for the major system components:

1. Preclude deferred ordering of data that is only utilized in the performance of a contract and/or for a period longer than the statutory period.
2. Require that the deferred ordering of data necessary for segregation or reintegration purposes be made only in response to a specifically identified and objectively reasonable segregation/reintegration need, be accompanied by a clear articulation of the nexus between the ordered data and the need, and be done only after consideration of all other alternatives (such as the use of form, fit and function data, reverse engineering, and other strategies as outlined in DFARS 227.71 03-5(d)(2)).
3. Provide guidance for negotiating certain cases in which it is appropriate to carve data out of deferred ordering (e.g. DMPD regarding a privately developed black box/LRU).
4. Provide guidance on appropriate use of deferred ordering in basic and applied research contracts.
5. Encourage programs to provide a feedback mechanism to learn lessons from circumstances when deferred ordering is used, for the purpose of improving program management best practices, and training to minimize the use of deferred ordering in future cases.

The panel also recommends DoD consider establishing internal approval protocols for agreements with contractors to exempt certain types of data from deferred ordering.

24 Deferred ordering period: 6 years (rather than perpetual) and Deferred Ordering Part 1: only data “generated” under the contract (Minority Position)

Issue

Some industry panel members and one Government member suggested a legislative proposal to further restrict the Government’s right to deferred ordering, by adding to the statutory language at 10 USC 2320(b)(9), “and except for data (other than data described at paragraphs (A) and (G) of subsection (a)(2)) that the government and the contractor have agreed will not be subject to deferred ordering.”

Proposal

Initially, industry members proposed to make deferred ordering “optional” for all contracts. Lacking consensus for this position, they proposed to make the clause optional for contracts with “mixed funding”. They argued that this clause will have a “chilling effect” on innovative technology and the development of new products, particularly as it relates to nontraditional companies, which generate most of the technological innovation.

Minority Proposed Compromise: The minority members agree with Congress that the clause should be mandatory in most instances, in order to provide DoD the flexibility it requires to better support the warfighter, in a dynamic environment. To obviate the need for a “minority report”, several Government members of the Panel proposed a compromise – to limit the application of the deferred ordering to the “traditional” defense contractors, and to make the clause “optional” for the nontraditional companies.

The compromise language for 10 USC 2320(b)(9) would be: “and except for data (other than data described at paragraph (A) and (G), subsection (a)(2)) that the government and a nondefense contractor have agreed will not be subject to deferred ordering.”

Minority members also proposed to add the definition of “nondefense contractor” at 10 USC 2320(g) as follows: “nontraditional defense contractor as defined under section 2302(9) of this title, or any other contractor as defined in regulations prescribed by the Secretary of Defense.”

Industry Reaction to Compromise: Industry members of the Panel immediately rejected this compromise. They reiterated their position to make deferred ordering optional for all defense contracts, including contracts with large, established defense contractors.

Legislative History: Congress has amended the defense technical data rights statute twice in the last six years, to narrow the circumstances under which DoD may invoke the deferred ordering

clause in its contracts. It has not taken any action regarding the FAR deferred ordering clause, which has been undisturbed for thirty years.

Prior to enactment of Pub. L. 112–81, § 815(a)(2), 31 December 2011, defense and civilian agencies, through the public rulemaking process, implemented deferred ordering clauses at DFARS 252.227-7027, Deferred Ordering of Technical Data or Computer Software (APR 1988), and FAR 52.227-16, Additional Data Requirements (Jun 1987), respectively.

Pub. L. 112–81, § 815(a)(2) narrowed the Government's ability to exercise deferred ordering by imposing a requirement for a Government determination that the technical data is needed for a particular Government purpose (e.g., reprocurement, sustainment, modification, or upgrade) and the technical data pertained to an item or process developed in whole or in part with Federal funds or was necessary for segregation or reintegration purposes. At the same time, the statute broadened the Government's ability to exercise deferred ordering by expanding the time period to “at any time” and by adding technical data “utilized in the performance of the contract” to the scope of deferred ordering.

Industry lobbying caused Congress in Pub. L. 114–328, § 809(c), 23 December 2016, to again narrow the Government's ability to exercise deferred ordering by further amending the DoD technical data rights statute by reducing the ordering period from “at any time” to “six years” and by removing technical data “utilized in the performance of the contract” (similar language in the Civilian deferred ordering clause, e.g., “specifically used in the performance of this contract” remains undisturbed).

Discussion

Recently, industry has complained to Congress that the “Deferred Ordering” clause (DFARS 252.227-7027) was unworkable and a disincentive to innovative companies participating in defense contracts. However, it has not provided specific examples of the unworkability of the clause or examples where firms have actually declined to participate in DoD contracts that include DFARS 252.227-7027. As indicated above, industry proposes “optional” use of the clause and vigorously opposes making this clause mandatory.

Under the auspices of this Panel, industry seeks again to further narrow DoD's ability to exercise deferred ordering, proposing that the Government and the contractor agree to exclude from deferred ordering any technical data developed with mixed funding including interfaces. The industry panel members allege that this narrowing of deferred ordering is necessary to attract innovative companies, and to protect the private funding that is present in a mixed funding scenario. They also allege that deferred ordering is not needed if the parties agree at the onset what level of data rights will be needed by the Government for sustainment purposes. The Government members, meanwhile, have repeatedly made clear that such negotiations are aimed at limiting the Government's flexibility later, in the life cycle of the weapon system, when more is known about sustainment. The proposed exclusion will limit that flexibility even more, and will restrict DoD's ability to support the warfighter.

This limitation will become most manifest in how the segregability rule will soon be employed. Industry panel members refuse to accept the solution provided by Congress to limit deferred ordering to technical data related to Government funding and do not discuss how their regulatory right to segregate items will tilt the bargaining power irretrievably to their side, in a defense acquisition. By opting to make segregability determinations at a higher level in the system architecture, contractors can maximize mixed funding scenarios and avoid deferred ordering altogether.

Industry panel members also do not address the statutory requirement in 10 USC 2320(a)(1) to define the “**legitimate interest of the United States**” and of a contractor or subcontractor in technical data pertaining to an item or process by ignoring any legitimate interest of the United States in protecting the warfighter’s need for technical data for field sustainment during combat operations.

Bottom Line: Industry’s proposal substantially decreases industry’s risk and maximizes its profit margin while it critically increases DoD’s risk for organic sustainment of its weapon systems, and adversely impacts readiness. At contract award, neither industry nor the Government know exactly which data will be required for sustainment purposes several years into the future. **Without the right to deferred ordering, DoD would have no leverage to negotiate a fair and reasonable price for the data it requires to support the warfighter. It would be at the mercy of the contractor to determine whether it will share the required data and if so, at what price.**

In a recent article, “*Get off the Hamster Wheel & Fix Readiness*”, the Army Chief of Staff, Gen. Mark Miley and the AMC Commander, Gen Gus Perna, address the impact of technical data rights on readiness. “*Owning data rights will also improve readiness, Perna said, at least for frontline equipment that must go places that contractor service representatives can’t.*” He went on to say that in Iraq and Afghanistan, the Army became dependent on contractor personnel to do even routine maintenance but troops will have to leave the civilian contractors behind and keep their gear in working order themselves. “*To do that properly, they need full access to the technical data.*”

<https://breakingdefense.com/2017/11/get-off-the-hamster-wheel-fix-readiness-amc-commander/>

INDUSTRY HAS MANY AVENUES TO AVOID DEFERRED ORDERING

1. Industry may simply make segregability determinations, at the lowest practicable level to avoid mixed funding determinations.
2. Industry may choose to avoid use of Government funding for a particular component, even if that component is required by the contract, so only industry dollars are used for that development.
3. Industry may avoid deferred ordering by employing a different contractual instrument, such as cooperative agreements (CAs), cooperative research and development agreements (CRADAs), or other transactions (OTAs). None of those agreements have mandatory deferred ordering, and they can be used to turn prior Government investments into private funding under the DFARS.

PROPOSED LANGUAGE UNDULY LIMITS SECRETARY OF DEFENSE FLEXIBILITY REGARDING CORE LOGISTICS CAPABILITY DETERMINATIONS

Let's illustrate how these rules will impact DoD acquisitions with an actual example. In the recent past, an Air Force acquisition program adopted an innovative technology into the product baseline. The acquisition strategy was based on a small quantity assumption. Due to small number of items to be acquired, analysis demonstrated that organic sustainment was more expensive than contractor sustainment. The item was fielded, and was so successful, that it transitioned to an ACAT ID program with much larger quantity of items. DoD also made a core capability requirements determination subsequent to Milestone C. Due to the much larger number of items, the new analysis determined that organic sustainment was much cheaper than contractor sustainment. However, the Government did not possess the appropriate data nor the rights to the data for organic sustainment. (Contractor ultimately allowed a limited amount of organic sustainment, as it was unable to provide timely sustainment on that scale.)

This proposed statutory change would exacerbate instances like the above scenario for exactly the types of technology DoD is hoping to attract.

PROPOSED LANGUAGE UNDULY LIMITS MOSA (Modular Open Systems Approach)

The proposal purports to add flexibility by providing authority to exempt from deferred ordering certain data, i.e., development with mixed funding at (a)(2)(E), and interfaces developed with mixed funding at (a)(2)(F). A key concept of MOSA is the balancing of a contractor's proprietary rights in "black boxes" against a Government statutory requirement for competition and the prevention of "vendor-lock." The Government may meet its obligations under the Competition in Contracting Act by maintaining rights in interfaces, so the contractor's "black box" may be replaced pursuant to a competitively-awarded contract with another "black box" item that is available in the marketplace.

Yet, by exempting from deferred ordering interfaces developed with mixed funding, the Government will find itself in a "vendor-lock" situation later in the acquisition life cycle. This industry proposal will decrease the likelihood that the "DoD does not pay more than once for the same work," and reduces the likelihood of "cost-effective re-procurement, sustainment, modification, and upgrades to Department of Defense systems."

PROPOSED LANGUAGE UNDULY LIMITS SMALL BUSINESS PARTICIPATION

In stark contrast to industry's inability to identify specific examples in support of its proposal, the Panel has received comments from MARPA (Modification and Replacement Parts Association) that the lack of technical data prevents the Government from awarding small business contracts for maintenance and sustainment and impairs the re-procurement of spare parts, at a competitive price. However, if we maintain the right to deferred ordering, the Government can mitigate this situation to a great extent, by ordering the necessary data when required.

An October 24, 2016 Reuters article “*Boeing takes on peers, partners in bid for replacement parts business*” supports MARPA’s position that OEMs foreclose competition in the spare parts market, “in search of higher profits margins, Boeing is focused on increasing market share in the “lucrative market for replacement parts and repair services.”

PROPOSED LANGUAGE UNDULY LIMITS COMPETITION

This lack of technical data has allowed a certain defense contractor to operate “as a hidden monopolist” and engage in price gouging by raising the price of proprietary aerospace spare parts, such as vibration panels and motor rotors, by over 800%. Many sole source contracts and the additional costs of those contracts result from a lack of technical data. The Government should not willingly accommodate a statutory change that is likely to result in increased vendor-lock and sole source contracts.

FLEXIBILITY FOR FLEXIBILITY’S SAKE IS NOT A POLICY GOAL

Industry panel members purport that their proposal enables additional “flexibility” in the acquisition. However, Government has sufficient flexibility regarding deferred ordering. No justification has been provided as to the benefits of that flexibility in a FAR/DFARS context. As indicated previously, appropriate flexibility already exists with CAs, CRADAs and OTAs where deferred ordering does not apply.

GOVERNMENT CANNOT PREDICT THE FUTURE

Contracting officers and program managers are forced to make tradeoff decisions during the development phase of weapons systems in order to maintain cost, schedule and performance. These decisions are necessarily focused on short term contingencies, in part because the budget pressures on any given program are intense. In order to field cutting edge capability, trade-offs must be made. In shouldering the vast majority of the risk in these acquisitions, the Government should be afforded the flexibility to meet the life cycle needs of the weapon system.

However, the impact of a decision to forego technical data cannot be quantified until decades after that decision is made. Even a well thought-out acquisition strategy, based on facts known at the time of the acquisition, may have an adverse impact on the warfighter because the defense realm is so dynamic that it would be impossible to predict our needs accurately. For example, a decision to trade off technical data in a cooperative agreement, TMRR contract, or an EMD contract is unlikely to adversely impact the buying activity making that decision. However, it may have adverse impact on the sustainment of the system, decades later.

In addition to the above, if we have to determine level of data/data rights required going into EMD, we would most likely request the broadest possible acquisition of data because we would not yet know what subsystems or components will ultimately be brought into the organic infrastructure. Deferring the ordering until later (past PDR or even CDR), is essential for the Gov’t to satisfy the intent of the policy set forth in DFARS 227.7103-1 “to acquire only the technical data, and the rights in that data, necessary to satisfy agency needs.” Once the design of

the item is more mature, we can make a more informed decision of our specific tech data needs and tailor it accordingly.

Recommendation

We urge the Secretary of Defense to **non-concur** on the statutory proposal to make deferred ordering optional, in his recommendations to the congressional defense committees for the following reasons:

- The proposal unduly increases DoD's risk regarding organic sustainment of its weapons systems and future competitive procurements
- The proposal unduly limits DoD implementation of MOSA
- It unduly limits small business participation in defense contracts
- It unduly increases vendor-lock which will exacerbate the price gouging that DoD has experienced and will continue to experience for the foreseeable future.
- It does not serve the needs of the warfighter in the dynamic realm in which DoD operates.
- It does not serve the interest of the American taxpayer.

25. Time Limits on Priced Contract Options

Tension Point

The period to exercise contract options for data/data rights is often not sufficiently long to ensure major systems and subsystems are properly sustained.

Issue

10 USC 2320(e)(1)-(4) requires program managers for major weapon systems and subsystems of major weapon systems to assess the long-term technical data needs of these systems and establish acquisition strategies that provide for technical data rights needed to sustain the systems over their life cycle. Paragraph (e)(2) directs that the acquisition strategies “address the merits of using a priced contract option for the future delivery of technical data that were not acquired upon initial contract award.”

However, the duration of such contract options under typical contracting scenarios may be too short to address the long term uncertainty of potential changes in the sustainment plan. More specifically, 10 USC 2304a(f)¹ and DFARS 217.204 direct that contract options may have a period of up to five years. Options may be extended for additional periods, however, they cannot exceed 10 years without the written determination by the head of the agency that “exceptional circumstances” require a longer period. Exceptional circumstances is a difficult threshold to cross. “...period up to five years and may extend the contract period for one or more successive periods pursuant to an option provided in the contract or a modification of the contract. The total contract period as extended may not exceed 10 years unless such head of an agency determines in writing that exceptional circumstances necessitate a longer contract period.”

Discussion

These periods of time (e.g., 5 or 10 years) may not be sufficient for contracts which contain priced options for technical data rights because often the period of performance of the basic contract will have expired before the Government has sufficient information (e.g., potential changes to the sustainment plan to determine whether to exercise the options for additional data or data rights. In some cases, the use of the “exceptional circumstances” pathway may be available, but the use of this mechanism does not appear to be used consistently across various DoD components, and the need for longer term options for technical data may be so prevalent as

¹ 10 USC 2304a(f) Contract Period.-The head of an agency entering into a task or delivery order contract under this section may provide for the contract to cover any period up to five years and may extend the contract period for one or more successive periods pursuant to an option provided in the contract or a modification of the contract. The total contract period as extended may not exceed 10 years unless such head of an agency determines in writing that exceptional circumstances necessitate a longer contract period.

to argue that it should be treated a more routine approach, rather than being “exceptional circumstances.”

To encourage more consistent use of priced contract options with sufficient duration to address long-term sustainment needs, including changes in the sustainment plan, the statutory coverage should be revised to more clearly encourage the use of such mechanisms.

The Government panelists believe that the contract options for data/data rights should be available for a period of time not to exceed (NTE) 20 years and that the options should include the level of rights needed to organically or competitively sustain weapon systems and subsystems over their life cycle.

Further, the panelists believe that the approval level for an option NTE a 10-year ordering period should be one level above the contracting officer. The approval level for an option NTE 20-years should be the Head of Contracting Activity (HCA). Such priced options should include an economic price adjustment (EPA)

Recommendation

1. The panel recommends the following change to Title 10 U.S.C. 2320(e)(2):

(2) **to the extent practicable, require the use of appropriate contract mechanisms (e.g., address the merits of including a priced contract options, not to exceed 20 years; escrow arrangements) for the future delivery of technical data and associated license rights** that were not acquired upon initial contract award **but may be necessary to support the life cycle sustainment plan;**

(3) address the potential for changes in the sustainment plan over the life cycle of the weapon system or subsystem; and

(4) apply to weapon systems and subsystems that are to be supported by performance-based logistics arrangements as well as to weapons systems and subsystems that are to be supported by other sustainment approaches.

2. The Panel recommends the following Regulatory changes:

a. DFARS 217.204 (ii), add:

(F) Priced Contract Options for technical data and computer software or associated license rights

b. DFARS 217.204 (iii), add:

For options not to exceed 10 years, obtain approval at least one level above the contracting officer.

For options not to exceed 20 years, obtain approval from the Head of Contracting Authority (HCA). This authority may be delegated by the HCA, no lower than one level above the contracting officer.

- c. DFARS 204.1601(c)(i) add (E), to allow closeout of the predecessor contract and maintain the option period, for technical data matter only, in the continued contract.
- d. DFARS 227.71 & .72 include a cross reference to DFARS 204.1601(c)(i)(E).

26. Deferred Ordering Part 2: all interface or major systems interface data may be ordered regardless of U.S. Government development funding

Tension Point

Recent legislation has mandated and expanded Deferred Ordering for certain types of Interface Data in a way that substantially increases risks for contractors.

Issue

Defense Federal Acquisition Regulation Supplement (DFARS) 227.7103-8(b) prescribes using the Deferred Ordering clause (DFARS 252.227-7027) when a firm requirement for a particular data item(s) has not been established prior to contract award but there is a potential need for the data. Under the clause, the contracting officer may order any data that has been generated in the performance of the contract or any subcontract thereunder at any time until three years after acceptance of all items (other than technical data or computer software) under the contract or contract termination, whichever is later.

Fiscal year (FY) 2012 National Defense Authorization Act (NDAA) added¹ a version of deferred ordering to the list of contract provisions required “whenever practicable” under 10 U.S.C. 2320(b) upon a determination that—

- (A) the technical data is needed for the purpose of reprocurement, sustainment, modification, or upgrade (including through competitive means) of a major system or subsystem thereof, a weapon system or subsystem thereof, or any noncommercial item or process; and
- (B) the technical data... (ii) 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...

While this has yet to be implemented in the DFARS, FY2017 NDAA² replaced subparagraph (B)(ii) with, “is described in subparagraphs (D)(i)(II), (F), and (G) of subsection (a)(2).” This correlates to technical data pertaining to:

¹ Section 815(a)(2)(C)

² Section 809(c)(1) and (2).

- 1) an interface between an item or process and other items or processes 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, in which case the release of limited rights technical data to, and use of such data by, persons outside the Government is authorized;³
- 2) an interface between an item or process and other items or processes that was developed in part with Federal funds and in part at private expense, in which case the United States (US) shall have government purpose rights (GPR);⁴
- 3) a major system interface (MSI) developed exclusively at private expense or in part with Federal funds and in part at private expense and used in a modular open system approach (MOSA),⁵ in which case the US shall have GPR.⁶

Technical data falling into either category 1 or 3, above, can be deferred ordered even if it was developed entirely at private expense.⁷ Technical data in category 2 also bears no relation to the funding for the development of the item being interfaced.

The lack of connection to funding is entirely inconsistent with the current law as understood by industry. And while the MSI concept is defined in the MOSA statutes, there is no such definition for a generic interface, no limit on the depth at which such an interface can reside (i.e., it is not limited to external interfaces at the sub-system level), and therefore nothing preventing it from being applied to internal interfaces within a technology provider's "black box." These provisions will require commercial subcontractor/supplier to cede (and prime contractors and higher-tier suppliers to obtain on the Government's behalf) rights in commercial interface data (and potentially, rights in commercial software interfaces such as application programming interfaces) that vastly exceed what customarily is provided in the commercial marketplace. Altogether, the concern is that the deferred ordering provisions, combined with the augmented US rights, could severely undermine the trade secrets that might reside in those interfaces.

There also is no exemption for commercial proprietary interface data (the commercial equivalent of "limited rights data"). According to recent practice,⁸ it is expected that the DFARS deferred

³ Section 809(b)(3)

⁴ Except in any case in which the Secretary of Defense determines, on the basis of criteria established in the regulations, that negotiation of different rights would be in the best interest of the US. Section 809(b)(5).

⁵ Pursuant to 10 U.S.C. 2446a.

⁶ Except in any case in which the Secretary of Defense determines, on the basis of criteria established in the regulations, that negotiation of different rights would be in the best interest of the US. Such MSI shall be identified in the contract solicitation and the contract. Section 809(b)(5).

⁷ In the case of an MSI developed exclusively at private expense and falling into category 3 but not 1, the DoD shall negotiate with the contractor the appropriate and reasonable compensation. Section 809(b)(5).

⁸ In the recently published proposed DFARS rule to implement Section 815 of the FY12 NDAA (DFARS Case 2012-D022), DoD has proposed to make the deferred ordering clause a mandatory flow down to essentially all

ordering clause at 252.227-7027 would become a new mandatory flow-down clause to commercial subcontractors and suppliers, even though the current clause has been expressly applicable only to “noncommercial items or processes” since at least 1988 (see DFARS 227.7103-8). If so, the result could significantly disrupt commercial operations, substantially increase the prices paid for commercial items and create a barrier to attracting commercial and non-traditional contractors to doing business with the Department of Defense (DoD). Industry believes that the foregoing statutory provisions provide overly broad authority for the release or disclosure of technical data related to interfaces below the first-tier subsystem level.

Recommendation

The Panel recommends no change to 10 U.S.C. 2320 or 10 U.S.C. 2321 to address this issue.

The Panel reiterates the recommendations from papers 11, 24, 29 and 30 pertaining to:

- definitions of interface data necessary for segregation and reintegration and of data pertaining to an interface,
- guidelines regarding what constitutes development of an interface,
- requirements, to the maximum extent practicable, prior to contract award, to specify by mutual agreement—
 - the required nature and character of that data that will be subject either to limited-rights-exception release/use or to GPR regardless of funding; and
 - delivery requirements for that data, addressing contingency-based needs through other preferred mechanisms (e.g., priced contract options, escrow, bilateral contract modifications);
- guidance for negotiating certain cases in which it is appropriate to carve data out of deferred ordering (e.g., detailed manufacturing or process data regarding a privately developed black box/LRU); and
- encouraging program managers to provide a feedback mechanism to learn lessons from circumstances when deferred ordering is used, for the purpose of improving program management best practices, and training to minimize the use of deferred ordering in future cases

In addition, the panel recommends the following changes to the implementing regulations to:

- 1) Provide the owner of the segregation/reintegration interface data an express right to redact technical data or computer software to exclude any content not necessary for segregation/reintegration in its response to a deferred order, pursuant to 10 U.S.C.

subcontracts and supply agreements at all tiers, including for commercial subcontractors and suppliers for commercial items used in any weapons system.

2320(b)(9)(B)(ii), with cost of such redaction being incorporated into the cost of converting the data into the Government's format.

- 2) Require that the deferred ordering, pursuant to 10 U.S.C. 2320(b)(9)(B)(ii), of interface data necessary for segregation or reintegration purposes be made only in response to a specifically identified need to segregate or reintegrate the item or process referred to in 10 U.S.C. 2320(a)(2)(D)(i)(II), and clearly articulate that need to the contractor.

27. Failure to Define and Order CDRLs (Reliance on Deferred Ordering and DAL to Obtain Data)

Tension Point

While DoD guidance requires upfront identification of necessary data deliverables, the increased use of deferred ordering to later acquire additional data leads to unnecessary contractual uncertainty.

Issue

The Panel received considerable comments on the effects of failure to order upfront data needed for the DoD to perform its functions. The Panel also notes that 10 U.S.C. § 2320(b)(2) through (4), implemented in DFARS 227.7103-2 & 227.7203-2, require government officials to plan and acquire data using contract line-items (“CLINs”) and specific contract requirements. 10 U.S.C. § 2320(b)(9) also requires a clause, currently in DFARS 252.227-7027, which provides for ordering data not specified in the contract.

Discussion

Industry comments indicate that they are seeing contracts where the listing of any data on a Data Accession List (DAL) gives rise to an obligation to deliver that data. These two provisions create a conflict since the combination gives the impression that even without going through rigorous data planning required by DFARS 227.7103-2 & 227.7203-2, the program can always fall back on mechanisms which allow for later ordering of any needed data.

Government does not dispute the need to specify deliverables in the contract, but instead notes that there are major consequences for a failure to order data, including failure to execute programs, the inability to compete follow on contracts, and the inability to sustain items for the product lifecycle. As such, DFARS has a deferred ordering clause for use with technical data or computer software generated under the contract, and has been using the DAL as an ordering menu for later ordering program data generated under the contract.

While industry comments generally objected to these sorts of provisions, of special concern was a belief that such clauses are used to counter deliberate Government and contractor agreements in contract. In these situations, contractors have relied upon mutual agreements, set up their supply chains and priced their contracts accordingly. Where the Government has not ordered such data, the Government and contractor would enter into a separate contract action which

fairly compensates the contractor and any applicable supplier. As such, industry comments note that the presence of deferred ordering or DAL practices induce risk into the process, and this risk is more acute where the contractor has relied on a limited set of deliverables in order to enter into the contract. For this reason, industry has called for the repeal of 10 USC 2320(b)(9) so that deferred ordering clauses would no longer be considered mandatory.

The current regulations do not recognize any consequence for ordering data using deferred ordering or the DAL, which undermines the requirements of 10 U.S.C. §§ 2320(b)(2) through (4). Industry commenters note that, in addition to undermining contractual clarity, these requirements also ensure that the Government obtains the exact data it needs for a program, regardless of contract, whereas the terms and conditions for the DAL and deferred ordering trigger deliverables based on when data is generated. In this sense, this is a contractual failure which needs to be tracked and root cause corrected.

One Government comment indicated that a failure to order can often be traced back to Government personnel simply not knowing what the applicable technical data items are called. As an example, the comment noted that a data acquisition planner cannot order a control drawing if they do not know what it is, or what that type of drawing is used for under ASME Y14.24. Industry has also commented on the need for an update to Department guidance on data ordering, as well as ensuring that the IP Strategy in DoD Instruction 5000.02 provide guidance as to what data to order, and when.

Recommendation

The panel recommends no statutory changes to U.S.C 2320 or 2321.

The Panel recommends that DFARS 227.7108 be revised to include guidance regarding integrated data environment (IDE) and repositories.

The Panel proposes the Department should update DoD 5010-12M to provide more guidance on common types of data which are ordered at different stages, and to ensure data ordering is in accordance with an IP Strategy

The Panel proposes the Department should update DoD Instruction 5000.02 to require the IP strategy to address the approach to data ordering account for different scenarios for potential changes in lifecycle sustainment plans, and also provides a feedback mechanism to identify the root cause why-deferred ordering is invoked.

The Panel recommends that defense standardization office provide explanatory notes on the use of DIDs, eg...DI-MGMT-81453B is revised to mandate that ordering of any data from the DAL shall be in accordance with DFARS 252.227-7027.

Recommends PGI address best practice for any SOW that includes CDRLs

The Panel recommends that MIL HDBK 245D be revised to reference a CDRL and DID for each tasking statement pertaining to research, development, testing, and evaluation, when the government wants the data delivered.

28. Escrow as a Form of Deferred Delivery

Tension Point

The existing DFARS includes a deferred delivery clause, which allows later delivery of contract data, whereas escrow agreements provide additional flexibility which may make such agreements more useful

Issue/Discussion

The Panel received Government comments about problems related to transitioning work to second sources when the component OEM is no longer able to maintain the component or product. To mitigate this risk, Government practices would be to ensure that the data is ordered. However, such practices can reduce competition where contractors refuse to deliver such levels of data when it is most valuable to the company, and even if ordered, can also lead to the Government ordering data which becomes stale by the time it is needed. The Panel has also received Government comments that such requirements result in a tsunami of data, which create configuration management and storage issues which the program is not prepared for.

The Panel received industry comments that a common industry practice to mitigate this risk is to use escrow agreements. Such agreements provide for the delivery of complete technical data packages on specified events, and often can have requirements to ensure that the escrowed data is kept current. In this manner, the buyer cannot obtain or use the data while the supplier is actively selling the component or product, which provides the supplier its exclusive use of the data. Should the supplier go bankrupt or otherwise no longer supply the component or product at necessary levels, the buyer would have a licensed copy of the most up to date version of the data, which would also be configuration managed up to that point. The Panel is not aware of DoD regulations which prohibit the use of escrow agreements.

The Panel notes that the DFARS already includes a deferred delivery clause, DFARS 252.227-7026. However, this clause required delivery within two (2) years of acceptance of all items under the contract or contract termination and the obligation expires thereafter. As such, there is no standard clause which mirrors the escrow concept or terms and conditions.

Recommendation

The Panel does not recommend a statutory change to 10 U.S.C 2320 or 2321.

The Panel recommends that the DAR Council consider revising DFARS (e.g. 227.7108, 227.7103-8) to address the use of escrow agreements that allow delivery of specified data based on mutually agreed upon conditions, specify which entity will hold the data in escrow, who will pay for the escrow, the scope of any license to use, and ensure such data is updated as appropriate for configuration management. (CI/CSCI)

29. Government Purpose Rights (GPR) in Major System Interface (MSI) (Developed Exclusively at Private Expense (DEPE) or with Mixed Funding)

Tension Point

The FY2017 NDAA provides for GPR in technical data pertaining to major systems interfaces that are developed either exclusively at private expense or with mixed funding. Contractors face added risk and uncertainty as a result of providing GPR for anything developed exclusively at private expense, applying the funding test to interfaces rather than items or processes, and ambiguity regarding the level within a system at which the interfaces will be defined.

Issue

The FY2017 NDAA added¹ new subsection (G) to 10 USC 2320(a)(2), providing that the United States (US) gets GPR in technical data pertaining to a MSI that is (i) developed either exclusively at private expense or with mixed funding and (ii) used in a modular open system approach (MOSA). The terms MOSA and MSI, along with the terms major system platform and major system component, on which the terms MOSA and MSI depend, are defined in 10 USC 2446a.²

Discussion

New 2320(a)(2)(G) does require that such MSI shall be identified in the contract solicitation and the contract.³ While this requirement will resolve some of the ambiguity inherent in the definition of “major system component,” how it is applied will determine what rights the US is seeking in technical data pertaining to system elements potentially well below the first-tier subsystem level that are commercial or otherwise developed exclusively at private expense. For example, based on the statutory definition,⁴ a “major system component” could be either or both

¹ FY2017 NDAA, Section 809(b)(5).

² FY2017 NDAA, Section 805(a)(1). According to that section, the term “major system interface” (i) means a shared boundary between a major system platform and a major system component, between major system components, or between major system platforms, (ii) is defined by various physical, logical, and functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software elements, and (iii) is characterized clearly in terms of form, function, and the content that flows across the interface in order to enable technological innovation, incremental improvements, integration, and interoperability.

³ Section 809(b)(5).

⁴ Per Section 805(a)(1), a “major system component” (i) is a high level subsystem or assembly that can be mounted or installed on a major system platform through well-defined major system interfaces, (ii) can be hardware, software, or an integrated assembly of both, and (iii) includes a subsystem or assembly that is likely to have additional capability requirements, is likely to change because of evolving technology or threat, is needed for

of the following: (1) an on-board radar system that represents a high-level subsystem installed on a “major system platform” or (2) a data processor that represents a high level assembly within the on-board radar subsystem. This means that MSI to which the government would be statutorily entitled to GPR could be any or all of the following:

- The external interfaces that connect the on-board radar system to the platform or other subsystems
- The internal interfaces within the on-board radar system (i.e., “inside the black box”) that connect the data processor to other high-level assemblies such as the power supply, receiver, display, etc...

Assembly elements such as the power supply, data processor hardware and displays are often commercial-off-the-shelf (COTS) items. As such, new 2320(a)(2)(G) together with the requisite solicitation language, could result in a statutory mandate for contractors and commercial suppliers to relinquish broad GPR⁵ in technical data pertaining to MSI inside the black box.

As applied to commercial interface data and coupled with new Defense Federal Acquisition Regulation Supplement (DFARS), flow down requirements to commercial subcontractors and suppliers could significantly disrupt commercial operations, substantially increase the prices paid for commercial items and create a barrier to attracting commercial and non-traditional contractors to doing business with the DoD.

For example, prime contractors and higher-tier suppliers will be required to obtain, on the Government’s behalf, rights in commercial subcontractor/supplier interface data (and potentially, rights in commercial software interfaces such as application programming interfaces (APIs)) that exceed the scope of rights customarily provided in the commercial marketplace. Industry has expressed concern with the prospect of broad flow down language (requiring flow down both to subcontractors and suppliers, adopted from the DFARS data rights clauses at 252.227-7015 and -7037), especially insofar as it applies to “suppliers,” which include commercial suppliers operating under pre-existing, long-term commercial agreements that are not identifiable to any specific commercial sale or government prime contract. On a complex major weapons system such as a major IT system or a commercial derivative aircraft, there are hundreds, and in some cases, even a thousand commercial suppliers throughout the supply chain that sell commercial items that may ultimately be integrated into a major weapon system. Reopening the terms and conditions of hundreds of pre-existing commercial supplier agreements is disruptive to

interoperability, facilitates incremental deployment of capabilities, or is expected to be replaced by another major system component.

⁵ Per the DFARS, GPR enables the government to release or disclose technical data outside the government for any government purpose, and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose the data for any government purpose. Moreover, GPR converts to “unlimited rights” five years after the applicable contract commences.

commercial operations, will undoubtedly increase costs, and puts all other commercial terms and conditions, including pricing models, at risk.

New subsection (G) also requires that, for technical data pertaining to a MSI developed exclusively at private expense for which the US asserts GPR, the DoD shall negotiate with the contractor the appropriate and reasonable compensation for such technical data.⁶

This will give rise to another tension point related to the DoD's efforts to drive its costs lower and to meet its needs for depot level capability through the acquisition of IP rights, sometimes at a price that is below the value of those rights by tying the IP transaction to a product purchase transaction. If DoD attempts to extract GPR for below-market value, there will be the long term risk of discouraging both traditional and non-traditional DoD suppliers from making their innovation available to DoD, or continue to invest at current levels, or both – since GPR enables DoD to make such suppliers IP available to competitors in a manner that will typically destroy value. Providing an innovative company's IP to competing enterprises will usually reward non-investing companies and punish investing companies by providing sales and profits to non-investing companies, while reducing the risk-adjusted returns of the innovative companies; ultimately an investing company's enterprise value will diminish to the point that needed credit and investment is driven away.

Additional tensions arise from the provisions of the FY17 NDAA directing DoD to use widely supported consensus-based standards in MOSA.⁷ To the extent that an MSI is commercial standard, contractors will be unable to procure GPR on behalf of the USG.

⁶ Presumably, this compensation will be for rights (i.e., GPR) in the technical data rather than for the technical data per se.

⁷The first section of the law relevant to this discussion is Section 805 “Modular Open System Approach in Development of Major Weapon Systems.” The first reference in Section 805 is the following:

“(e) Milestone B.—A major defense acquisition program may not receive Milestone B approval under section 2366b of this title until the milestone decision authority determines in writing that—

“(1) In the case of a program that uses a modular open system approach—

“(A) The program incorporates clearly defined major system interfaces between the major system platform and major system components, between major between major system components, and between major system platforms;

“(B) Such major system interfaces are consistent with the widely supported and consensus-based standards that exist at the time of the milestone decision, unless such standards are unavailable or unsuitable for particular major system interfaces; and

“(C)The Government has arranged to obtain appropriate and necessary intellectual property rights with respect to such major system platform;”

The second relevant section in Section 805 is the following: “The Secretary of each military department shall—

“(1) Coordinate with the other military departments, the defense agencies, defense and other private sector entities, national standard-setting organizations, and, when appropriate, with elements of the intelligence community with respect to the specification, identification, development, and maintenance of major system interfaces and standards for use in major system platforms, where practicable;

Recommendation

The panel does not recommend any changes to 10 U.S.C. 2320 or 2321.

The panel recommends the following with respect to the implementing regulations:

1. Create separate definitions, in terminology which is understood by each industry, for “technical data pertaining to an” MSI based upon whether the interface is hardware or software.
2. Require that, to the maximum extent practicable, when an MSI is identified in a contract solicitation, the Government and contractor will enter into negotiations, prior to contract award, to specify by mutual agreement the required nature and character of technical data pertaining to each MSI that will be subject to GPR.
3. Require that, in defining major system components and MSIs in contract solicitations, the Government consider the IP implications on competition and innovation
4. With respect to MOSA interfaces below the subsystem level, encourage the use of (instead of GPR) specially negotiated license rights (SNLRs) tailored to meet the DoD’s actual needs.
5. Exempt commercial items, either COTS or modified in a manner consistent with commercial practices in the applicable industry, from the applicability and flow down of new 2320(a)(2)(G). Instead, the Government’s rights in commercial interface data and software should be consistent with rights granted in the commercial marketplace and in accordance with commercial best practices for the underlying commercial item to be procured.
6. To the extent that MSIs incorporate commercial standards and other widely supported consensus based standards, the standards themselves will not be subject to GPR.

The implementing regulations should also establish standards for negotiating compensation for obtaining GPR in technical data pertaining to a MSI developed exclusively at private expense (and SBIR per paper 21:

1. DoD pays appropriate and reasonable value for those rights; and

The valuation of such rights should consider IP valuation best practices and applicable industry standards and economic principles

“(2) Ensure that major system interfaces incorporate commercial standards and other widely supported consensus based standards that are validated, published, and maintained by recognized standards organizations to the maximum extent practicable;”

30. GPR in Interfaces Developed with Mixed Funding

Tension Point

The mandate, introduced in the FY2017 NDAA, that the United States (US) shall have government purpose rights (GPR) in technical data pertaining to an interface between an item or process and other items or processes that was developed with mixed funding¹ is overly broad.

Issue

According to new subparagraph (a)(2)(F) of 10 USC 2320, the rights in interface data are determined by the source of funding used to develop the “interface.” However, the interface between two hardware elements in a system cannot practicably be described as a “thing” or “widget” such as a bracket or mating plug in the simplest of terms. Instead, the interface is an abstract concept that refers to design features of a widget that affect the design features of another widget. In other words, for hardware items, the “interface” is not typically a “thing” that is developed with mixed funding, and technical data pertaining to the interface – such as an interface control document (ICD) – defines interface requirements so as to ensure compatibility between the two widgets and to provide an authoritative means of controlling the design of the interfaces.

Despite this threshold uncertainty – and unlike the companion concept of major systems interface (MSI), in which the US also gets augmented rights – there are no statutory definitions or limits to guide what qualifies as an interface to which the US is entitled to GPR. By way of comparison, the concepts MSI, modular open system approach (MOSA), major system platform and major system component (MSC), on the latter three of which the term MSI depends², all are

¹ Except in any case in which the Secretary of Defense determines, on the basis of criteria established in the regulations, that negotiation of different rights would be in the best interest of the US. Section 809(b)(5).

² Per FY2017 NDAA, Section 805(a)(1) an MSI is a specific interface between a MSC and other MSCs or a major system platform. An MSI is defined by various physical, logical, and functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software elements. An MSI is characterized clearly in terms of form, function, and the content that flows across the interface in order to enable technological innovation, incremental improvements, integration, and interoperability. In turn, an MSC (i) is a high level subsystem or assembly that can be mounted or installed on a major system platform through well-defined major system interfaces, (ii) can be hardware, software, or an integrated assembly of both, and (iii) includes a subsystem or assembly that is likely to have additional capability requirements, is likely to change because of evolving technology or threat, is needed for interoperability, facilitates incremental deployment of capabilities, or is expected to be replaced by another major system component.

defined in new 10 USC 2446a.³ Beyond these definitional constraints, in order for the US to obtain GPR it is required that the MSI be identified in the contract solicitation and the contract.⁴

In contrast, the term “interface” is provided no such definitional or contractual constraints. Without such limits, the statutory provisions provide overly broad rights to release or disclose technical data related to interfaces below the first-tier subsystem level. Faced with task of implementing the concept of technical data the is necessary for segregation or reintegration of an item or process, per Section 815 of the FY2012 NDAA, the recently released Proposed Rule⁵ interpreted such data as applying the lowest practicable segregable level, e.g., a sub-item or subcomponent level, or any segregable portion of a process, computer software (e.g., a software subroutine that performs a specific function), as providing more detail than form, fit, and function data, and as potentially including detailed manufacturing or process data or computer software source code. There are no constraints to prevent “interface” data from being interpreted at the same level. This raises the prospect that GPR will attach (and, per Section 809(c)(1) and (2) of the FY2017 NDAA, deferred ordering can reach) deep into the subcomponents or software that reside within a privately-funded “black box” or other proprietary item.

Further, even if applied outside the “black box,” the application could have significantly different impacts depending on whether the interface pertains to hardware or software. With reference to the above-noted definition of MSI, while interface data would be physically observable and measurable from the exterior of a hardware black box without revealing the construction of the hardware black box, such data would be more detailed and revealing in the software industry. Thus, even to the extent that the software industry uses the same terminology, the data used for an interface may be much more detailed in describing a software program element as compared to the data used to describe the physical and electrical connections of a hardware element.

There also is no exemption for commercial interface data (including interfaces pertaining to commercial items developed exclusively at private expense) or for interface data protected by SBIR data rights (see tension point paper 6.b). DoD has taken the position that the data rights pertaining to any portion of a commercial item that was developed in any part at Government expense are determined according to non-commercial items rules, with the rules pertaining to commercial items governing only the technical data pertaining to that portion of the commercial item that was developed exclusively at private expense.⁶ With this new statutory concept of an “interface” being developed with mixed funding, it is likely that any adaptation of a commercial item using any Government funds will be considered to implicate the non-commercial rules. If

³ FY2017 NDAA, Section 805(a)(1).

⁴ Section 809(b)(5).

⁵ Defense Federal Acquisition Regulation Supplement: Rights in Technical Data and Validation of Proprietary Data Restrictions (DFARS Case 2012-D022), published in the Federal Register on June 16, 2016 (the Proposed Rule).

⁶ DFARS 227.7102-4(b)

recent practice⁷ is an indication, it is expected that the non-commercial data rights clauses would become a new mandatory flow-down clause to commercial subcontractors and suppliers. If so, the result could significantly disrupt commercial operations, substantially increase the prices paid for commercial items and create a barrier to attracting commercial and non-traditional contractors to doing business with the DoD.

For example, prime contractors and higher-tier suppliers will be required to obtain, on the government's behalf, rights in commercial subcontractor/supplier interface data (and potentially, rights in commercial software interfaces such as application programming interfaces (APIs)) that exceed the scope of rights customarily provided in the commercial marketplace. Industry has expressed concern with the prospect of broad flow down language (requiring flow down both to subcontractors and suppliers, adopted from the DFARS data rights clauses at 252.227-7015 and -7037), especially insofar as it applies to "suppliers," which include commercial suppliers operating under pre-existing, long-term commercial agreements that are not identifiable to any specific commercial sale or government prime contract. On a complex major weapons system such as a major IT system or a commercial derivative aircraft, there are hundreds, and in some cases, even a thousand commercial suppliers throughout the supply chain that sell commercial items that may ultimately be integrated into a major weapon system. Reopening the terms and conditions of hundreds of pre-existing commercial supplier agreements is disruptive to commercial operations, will undoubtedly increase costs, and puts all other commercial terms and conditions, including pricing models, at risk.

Recommendation

To clarify the requirement, amend 10 USC 2320(a)(2)(F) as follows:

Delete the following:

technical data pertaining to an interface between an item or process and other items or processes that was developed in part with Federal funds and in part at private expense

and insert the following:

technical data pertaining to an interface (between an item or process and other items or processes) that was developed in part with Federal funds and in part at private expense

in its place.

The panel recommends the following regulatory changes:

⁷ In the Proposed Rule, DoD has proposed to make the data rights clauses mandatory flow downs to essentially all subcontracts and supply agreements at all tiers, including for commercial subcontractors and suppliers for commercial items used in any weapons system.

1. Similar to the companion concept of major systems interface (MSI), define (with reference to the statutory definition for MSI) what qualifies as an “interface” and place limits on the level within a system at which GPR attaches to interfaces.
2. To the extent practicable, in order for the US to obtain GPR it is required that “interface” be identified in the contract solicitation and the contract.
3. Provide guidelines regarding what constitutes development of an interface. The guidelines should be tailored separately for software versus hardware versus processes, as appropriate.
4. Consider appropriate exemptions for commercial items, either COTS or modified in a manner consistent with commercial practices in the applicable industry, or for SBIR developed items, from the applicability and flow down of new 2320(a)(2)(F). Instead, the government’s rights in commercial interface data and software should be consistent with rights granted in the commercial marketplace and in accordance with commercial best practices for the underlying commercial item to be procured, and SBIR developed interface data should be covered by SBIR data rights.
5. Further tailor the definition of “interface” separately for software versus hardware versus processes

The panel also recommends the following:

ASD(R&E) provides guidelines regarding the nature, content and detail for specific documentation (e.g., an ICD) needed to define the boundary between specific classes of items. Where possible, the interfaces should be well-defined, open and published interfaces implementing known standards. Where such standards do not exist, the regulations should call for interfaces based on consensus based standards which form a boundary between components that are self-contained elements.

Establish a policy for identifying interface specification data at the appropriate system level, in order to avoid requiring contractors to relinquish GPR in such lower level interface data, regardless of the level at which standards have been developed. This will have no effect on the government’s rights in form/fit/function data.