INTELLECTUAL PROPERTY

Avoid vendor lock with rights to interfaces and operational data

Problem: MOSA can turn programs into "big bang" efforts with long lists of directed standards, asking for data and license rights to virtually everything

Recommendation: Rather than focus on specific standards, influence a microservices architecture with rights to interfaces and operational data

Principles:

- Communicate IP needs but don't let it bog down contracting while there's competition
- Focus on federated development rather than an inflexible consensus on global standards
- Order Interface Control Documents and Interface Exchange Requirements
- Enable on-demand translations between standards, e.g., STITCHES tool

Things to Consider:

- Setting up a CI/CD Pipeline with a software factory or FedRAMP vendor
- Containerize each app using well-defined interfaces
- Utilize an abstraction layer for hardware to speed up test
- Strategies for continuous testing
- Leverage latest open source tools

Success: Vendors can be onboarded quickly if needed, particularly at the application and data layers, and contractors can keep IP to their "black boxes"

Resources: FAR Part 27 and DFARS Part 227; DAU IP Guidebook Suite; DoD OTA Guide; SoS Technology Integration Tool Chain for Heterogeneous Electronic Systems

Context & Motivation

Not only is commercial spending on R&D far outpacing the government's own, a simultaneous trend has been a shift in sources of economic value from tangible to intangible capital. No longer is a company's competitive advantage found in its physical plant, equipment, and inventory. Instead, the competition is increasingly dominated by intangibles such as software, data, and product design. Back in 1975, these intangible factors only explained 17 percent of the S&P 500's valuation, the rest being found in tangible assets and earnings. By 2020 the intangibles accounted for 90 percent.

Unlike industrial goods, intangibles can be freely reproduced. The value is in the original idea and can easily spillover to the competition. "Information wants to be free," starts a common phrase, "but creators need to get paid." This explains why industry is "terrified of giving up IP rights" to government for meager revenue opportunities. Responses range from "our IP is our company" to "VCs don't want to touch a DoD contract because the IP might get out to the competition." IP is an important contributor to the fall of new entrants in defense contracting from 15,000 in 2010 to just 4,000 in 2019. If DoD wants the best commercial firms solving military problems, it will have to respect their primary asset—intellectual property.

At the same time, DoD must retain its unique needs for data rights. For example, most Web 2.0 firms like Facebook, Amazon, Apple, and Google have exclusive ownership of all the data their users generate. Those photos you post on social media don't belong to you. By contrast, DoD must have rights in critical mission data that contribute to the planning and execution of a war. Operational data is an enterprise capability, and that means accessibility to other defense organizations and even vendors.

Like many other aspects of acquisition, IP policies have seen a pendulum of reform. The recent standup of the DoD IP cadre and issuance of DoDI 5010.44 marks the latest swing towards increased guidance on technical and software data rights. The last major period started in 1984 with the enactment Title 10 US Code §2320 and culminated in the 1995 rule change to the DFARS that reflects today's regulation. In that time, the Packard Commission Report found that "suppliers have become alarmed by DoD's increasingly vigorous pursuit of unlimited rights in technical data to be used in fostering competition."

> "Government is so afraid of vendor lock that they drive away the vendors they need most."
>
> Contracting Officer

It seems the pursuit of IP gets exhausted due to the strains on contracting and the vendors outlasting or out-lawyering the government. By 2001, Congress held hearings on how IP policies were holding back innovation. DoD's guide on IP management stressed commerciality, specifically negotiated rights, and using performance-based acquisition to obviate the need for data rights.

IP issues laid dormant in the 2000s. The post-9/11 tranche of defense programs did not sufficiently plan for IP. After they went through a cycle of Nunn-McCurdy breaches between 2007 to 2013, the vendor-locked programs transitioned to the field. Defense officials found themselves unable to drive competition, perform organic maintenance, and access data. The Army led the charge with a Data & Data Rights Guide in 2015, followed by the Section 813 Panel initiated in the FY 2016 NDAA.

There exists a fundamental tension in IP guidance. DFARS 227.7103 and 227.7203 for non-commercial items directs DoD to only acquire the technical data and software data rights "necessary to satisfy agency needs." Usually this means deferring data rights acquisition to the latest point possible. By doing so, however, DoD loses leverage in negotiations. Therefore, guidance also requires lifecycle IP planning very early in program development, causing defense officials to protect themselves from uncertainty by requiring too many rights.

Modular Open Systems. The government has two major concerns with IP: avoidance of vendor lock and promotion of interoperability. In both of these cases, modular open systems architecture (MOSA) provides a theoretical remedy. A program could deconstruct the system into the relevant modules and create a systems map labeled according to whether it was government-funded, privately-funded, or used mixed funding. Using the open standards, government could "plug-and-play" modules, thereby improving competition and lessening the need for data rights. Open standards can also create enterprise efficiencies by fostering communication between systems and the sharing of components.

The problem, as discussed above, is that there is not enough information available at the development RFP stage to pre-specify standards. It can take a long time to reach a global agreement on a standard, and even then, it's hard to roll out across a diverse set of systems. The Air Force, for example, has used Link 16 for decades. It still isn't fully adopted and exists in several configurations. Locking in new standards, moreover, will not help existing programs that make up the vast majority of defense capabilities.

MOSA has met some success over the years—such as the Navy's Acoustic Rapid COTS Insertion effort, the Army's Ground Common Infrastructure Architecture, and the Air Force's OMS/UCI—but remains elusive as a global solution. This is indicated by renewed emphasis in law and guidance. Government officials must often resort to acquiring intellectual property to protect themselves where MOSA could not.

Fortunately, commercial firms have made a great deal of progress breaking down large, tightly integrated software systems. This has been achieved using architecture best practices in interface design, messaging syntax, document- -tation, and protocols for discovery. By contrast defense contractors often don't know their interfaces, requiring months to reverse engineer.

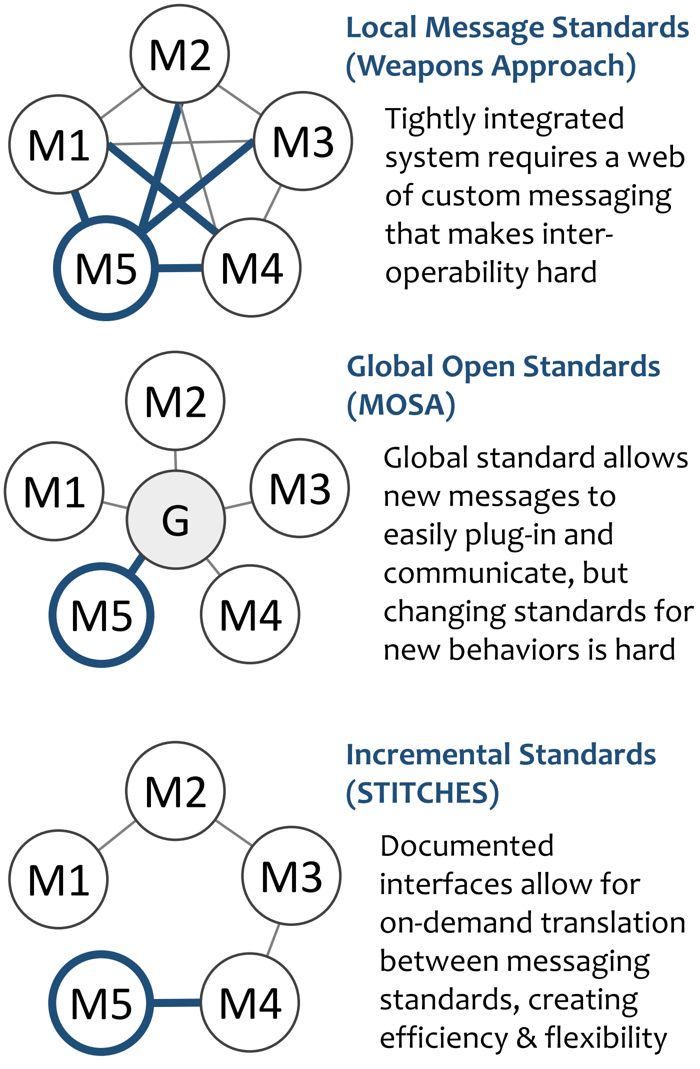
With documentation in hand, DARPA has also created a suite of tools including STITCHES which can create a translation between interfaces, supporting ad hoc interoperability (Figure 6). This means DoD programs do not have to slow down until a global consensus on standards is enforced, but can quickly swap modules or systems on-demand. As former deputy director of DARPA Dan Patt explained in plain language:

> "Maybe I shouldn't think about interoperability as trying to achieve a universal language. I shouldn't try to define Esperanto and force everybody to talk Esperanto. Maybe I should do on-demand translation—the Google translate equivalent… It might seem less elegant, but it's a lot more practical. And STITCHES is the equivalent of that, but for systems."

Mason GovCon's final play for software intensive systems seeks to protect the government's interests while reducing its need for intellectual property. Vendor lock can be avoided by using best practices for interface design as a criterion for progression through agile development. Ordering of data rights for the interfaces and operational data can be obtained when there is more information but before competition ends. Again, since there is no one-size-fits-all approach, we suggest two general tracks:

"First Mover" Strategies. When government is a "first mover," it is pulling commercial development along. Companies aren't bringing a lot of self-funded investment to the plate because the core technologies are not dual-use. In these cases, government should make clear its intent for acquiring more extensive data rights according to guidance. This is particularly true for government-led development such as occurs in defense labs and software factories.

"Fast Follower" Strategies. As more of defense systems are built from commercial technologies, the mixed funding rule leading to government purpose rights is overly restrictive. A company could have funded 99 percent of the technology and face losing their IP if the government invests just one percent. Long discussions might then occur on what is meant by a "readily segregable" work element (DFARS 27.408). When the government is acting as a "fast follower," it should avoid acquiring data rights until its ready to move forward on a major contract associated with a program of record.



Local Message Standards (Weapons Approach)

Tightly integrated system requires a web of custom messaging that makes interoperability hard

Global Open Standards (MOSA)

Global standard allows new messages to easily plug-in and communicate, but changing standards for new behaviors is hard

Incremental Standards (STITCHES)

Documented interfaces allow for on-demand translation between messaging standards, creating efficiency & flexibility

Figure 6. Comparison of System Messaging Standards [Source]

Treat Nontraditionals Differently. A major complaint of startups and commercial companies is that their self-funded IP is at greater risk than the taxpayer-funded IP investment made by traditional primes. As one small business association representative remarked: "… government practice attempts to acquire intellectual property and fails to do so in most large procurements, but does acquire intellectual property when contracting with small, innovative high-technology firms or outside commercial firms."

Government's hands are not tied when contracting with nontraditionals. Flexible IP is one of the primary reasons Congress gave DoD Other Transactions authority when research and prototyping is required. Since contracts with any nontraditional business unit can use commercial item procedures (DFARS 212.102), government can follow FAR 12 and commercial data rights and licensing terms (DFARS 227.7102 and 227.7202). Title 10 US Code §2320 also favors specially negotiated licenses.

Communicating IP needs. Contract solicitations should not include blanket requirements for government purpose rights, but rather specify the government's objectives for data rights. For example, the government may need the ability to swap an application with a competitor. The contractor could propose adopting open standards or it could provide data rights to custom interface documentation. For another example, the government may need to store data generated in military operations on a government specified cloud solution and share that data with other vendors. Hardware examples include the ability to perform organic maintenance and repair. These statements of use cases in solicitations allow the contractors to propose tailored solution that may be greater than limited or restricted rights but less than government purpose rights.

Source Selection. Most "first mover" strategies will use FAR 15 source selection procedures that are cumbersome. This includes the value adjusted total evaluated price process for determining best value. It requires adjusting the offeror's price based on the "value" of data rights included. Yet this method is fraught with difficulties in terms of valuation methods.

By contrast, "fast follower" strategies should veer towards contract procedures exempt from these source selection procedures, including FAR 16.505, FAR 8.4, FAR 13, and CSOs. Comparative evaluations require no ratings and provides a high degree of flexibility in evaluation and selection. Written evaluations can be streamlined and use on-the-spot evaluations. See the DHS PIL Bootcamp for more information on these approaches (Techniques 5 and 8).

Timing Data Rights. Today's "first mover" policies are geared toward early identification of IP needs and deferred delivery of the rights and data. Guidance suggests adding separately priced contract line item numbers to the contract. Competition in the development award incentivizes vendors to propose and reasonably price data rights. The government can exercise the option at its discretion. This practice works best for once-in-a-generation system that, after the development contract is awarded, loses competition.

A core idea of this playbook, particularly for software intensive systems, is modularizing large programs and iterating quickly. This means early contract awards are no assurance of large volume ordering, but are more likely initial experiments. At this stage, the government is not reliant on any contractor. It can influence open standards and documented interfaces along the way by maintaining competition. Only when government considers making a major purchase of the capability and down-selects to a single company is the government threatened by vendor lock. A successful development strategy should delay data rights negotiations to this stage when both parties in the relationship have something to lose. The vendor faces the loss of a major production contract while government faces the loss of competitive pressures.

Non-Disclosure Agreements. Government often needs delivery of the software code and documentation in the early phases of development in order to conduct testing. Rather than acquire data rights, a non-disclosure agreement (DFARS 227.7203-7) offers a model in line with commercial practices and provides a legal basis for enforcing confidentiality. This practice will help delay the acquisition of data rights.

Wrap Up. For software intensive systems, government has relatively low needs for data rights if it can keep competition open and enforce industry best practices in terms of documenting interfaces. Owning the operational data is also imperative to interoperability and enterprise-wise capabilities, but these rights can be delayed until production contracts and fielding. These considerations provide government a way to engage nontraditionals as a "fast follower."