Open-Source Software in Government Contracts

by Chad G. Clark | Jun 29, 2022 | Government Contracts, Intellectual Property Due Diligence

Chances are, if you find yourself reading this, you already know some of the ways open-source software (OSS) standards affect software development. Even so, developing software for the federal government presents its own special set of issues that are further complicated by OSS standards.

In this environment, companies must evaluate the government's ambivalence toward open-source software, as well as navigate the considerable challenges to protecting intellectual property (IP) when federal procurement regulations and OSS licenses apply.

A Love-Hate Relationship with OSS

When it comes to software procurement, the government has adopted a strongly pro-OSS stance. For example, recent policy guidance from the Department of Defense (DoD) chief information officer states that the DoD "must follow an 'Adopt, Buy, Create' approach to software, preferentially adopting existing government or OSS solutions before buying proprietary offerings."

For over a decade now, the DoD and other federal agencies have recognized the critical advantages provided by widespread use of well-vetted OSS. These advantages include rapid adaptability to new applications, robust, effective, and error-free code and lowered risk of vendor lock-in.

However, these advantages are potentially offset by two substantial risks that concern the DoD: 1) OSS can present an ingress point for malicious code, and 2) if improperly shared, OSS can allow adversaries to gain knowledge of national capabilities, limitations and vulnerabilities whose secrecy is vital to U.S. security interests.

Notwithstanding these potential drawbacks, the benefits of using OSS have led the DoD to deem all software "open by default" (i.e., releasable as OSS), with notable exceptions based on whether the

software:

- Was developed for "national security systems," meaning information systems supporting intelligence activities, cryptologic activities, military command and control or weapons systems
- Contains "critical technology," a broadly defined term including the categories of advanced command environments, persistent surveillance, power sources and management for distributed network sensors, high performance computing and defense-critical electronic components
- Is subject to export restrictions - practically, this means the software is subject to one or both sets of federal statutes governing International Traffic in Arms Regulation (ITAR), which regulate the sale, distribution and manufacturing of defense-related items, or Export Administration Regulation (EAR), which regulate dual-use items not directly covered by ITAR, but which still could be used in defense-related applications
- Is subject to use licenses that prevent release to the public

Although these exceptions can exempt software from DoD's OSS-by-default approach, unless the software delivered under contract is exempt, the contractor must provide it to the government as OSS.

The Exceptions Prove the Rule

Determining whether an exception applies isn't usually straightforward, not only because terms such as "critical technology" are broadly defined, but also due to funding-source issues emerging from the procurement contract itself. For example, many DoD software contract deliverables fall under the "national security systems" exception simply based on the tremendous demand for and high priority of projects in such areas. Similarly, the categories involved in software procurements may implicate "critical technologies," which are designated, on a per-project basis, by the project manager. Also, EAR/ITAR lists are quite extensive, further limiting the ability for the government to designate a software deliverable as OSS.

Limitations on the government's use rights can also prevent the delivery of software as OSS. For instance, absent an exception discussed above, if the government has "unlimited rights," it can release the delivered software as OSS. However, if a vendor funds some or all of the software's development cost, the vendor can limit some or all of the government's ability to release software as OSS.

For example, for DoD contracts, if the vendor privately funded part of the software development costs, the government may have "government purpose rights." Such rights only allow the government to release software to internal, government-only, open-source libraries, such as Redhawk SDR. "Restricted" and "commercial use" rights further constrain or prevent government's ability to release the software as OSS.

Is OSS Right for You?

Whether a company should allow its software to be released as OSS is a critical decision rooted in the

company's business model. Generally, to the extent the software is used to implement other company technology (e.g., UAV flight control software), the company should keep the software as proprietary. Likewise, software delivered directly to consumers (e.g., Microsoft Office, Adobe Acrobat, etc.), should also be maintained as proprietary.

By contrast, if software primarily facilitates access to other revenue streams, like how Google's search engine facilitates access to advertising revenue, OSS release is beneficial, allowing rapid innovation across many disciplines to support those streams. Similarly, software-as-a-service (SaaS) products are often initially released as OSS (either at no cost or for a nominal charge), while revenue from these services is generated from implementation or customization services.

It’s OSS, Not Philanthropy

Given the disclosure and licensing requirements associated with OSS, what, if any, IP protection strategies will work for OSS? This question is further complicated by the Supreme Court's Alice decision, as well as other federal court decisions following in the wake of Alice, which have led to post-issuance invalidations of a host of software-related patents.

As a result of the ongoing uncertainty arising from these cases, as well as the expense and rapid pace of software-related innovation, the use of patents to protect software innovation is now often impractical. However, if software-related innovations can be tied to unique or specialized technical systems (e.g., software that operates a wearable sensor suite), the use of patents remains a viable IP protection strategy, and the probability of obtaining a solid, software-related patent improves substantially by constraining the scope of the patent along these lines.

Despite the challenges, inventive software content can still be patented, and the creative aspects of OSS can still be copyrighted, bringing value to IP owners.

Patent and copyright coverage for OSS can provide a valuable backstop to better control rights surrendered when releasing innovative software as OSS. While OSS licenses may limit certain enforcement rights normally accruing to copyright and patent holders, OSS licensees may use their OSS licenses as a defense, where applicable, to unauthorized uses of software that uses OSS.

Additionally, offensive paths are available when others use a company's IP-rights-protected software without a license or if they violate the OSS license authorized for that software. In this way, IP legal protections can serve as a safety net, ensuring software innovations are used by others in more predictable ways, and preventing OSS from becoming a giveaway of hard-won innovation.

Contact:
Chad G. Clark
chad@martensenip.com
220-201-0051
Download vCard