



January 11, 2012

Defense Acquisition Regulations System
Attn: Mr. Mark Gomersall
OUSD(AT&L)DPAP(DARS)
Room 3B855
3060 Defense Pentagon
Washington, DC 20301-3060

Re: Public Meeting, DFARS – Open Source Software

Dear Mr. Gomersall:

The Aerospace Industries Association (AIA) appreciates the opportunity to provide comments to the questions listed in the "Notice of public meeting," that was published in the Federal Register on December 5, 2011 (76 F.R. 75875).

Responses to the Specific Questions

As to the list of specific questions on which the Government has expressly requested comment, we provide the following answers in Attachment 1.

Conclusion

AIA, on behalf of its member companies, thanks you for the opportunity to provide these comments. If you have any questions or need any additional information, please contact me at 703-358-1087 or susan.tonner@aia-aerospace.org.

Sincerely,

A handwritten signature in cursive script that reads 'Susan K. Tonner'.

Susan K. Tonner
Assistant Vice President
Acquisition Policy

Attachment

ATTACHMENT 1

Input Re: DoD Requests for Input Regarding Open Source Software Issues:

1. What are the risks that open source software may include proprietary or copyrighted material incorporated into the open source software without the authorization of the actual author, thereby exposing the Government and contractors who use or deliver the open source software to potential copyright infringement liability?

While the risk of inadvertently obtaining proprietary (non-open) source code is unknown, to date we have not seen a lot of copyright infringement or proprietary information misuse claims against open source providers. The SCO-Linux controversies over the past decade are the exception whereby the SCO Group alleged that its proprietary software code was improperly released under the GPL license in violation of its copyright. The lack of any other lawsuits may be in part because the developers who obtain this open source code obtain it directly from a site that makes the open source available, and provides only that code that software developers make available to those sites on an open source basis. These sites do not make available an integrated software solution composed of open source software and proprietary software. Actual users/developers of code, however, may have greater insight as to whether proprietary code is ever inadvertently included in the open source packages. In a number of instances, government contractors have found what could be unlicensed proprietary or copyrighted material in open source software.

Open source code is subject to copyright protection, and the standard open source licenses grant licenses under those copyright rights. Thus, all open source code contains copyrighted materials unless such code has been placed into the public domain – which sometimes occurs. Open source code generally does not contain other copyrighted “content” (for example, embedded text, artwork, music) that may be subject to separate copyright protection. Most open source that is used by industry for the performance of Government contract tends to provide basic functionality, utilities and libraries.

The greater risk of copyright infringement occurs when open source is distributed from one party to another party. Examples of distribution are when a Contractor delivers open source to the Government, or when the Government issues open source software to a Contractor as government-furnished software. Copyright infringement can also occur when software containing unauthorized third party software has been, unbeknownst to the contractor, incorporated into publicly available open source software and used by contractors. In such instances, contractors could not only incur significant liability for copyright infringement (e.g., statutory damages), but use and/or delivery of products to the Government could be stopped.

2. Are contractors facing performance and warranty deficiencies to the extent that the open source software does not meet contract requirements, and the open source software license leaves the contractors without recourse?

Yes, contractors are facing performance warranty deficiencies. In cases where open source software is the best, most efficient, least expensive solution, contractors may be forced to accept more liability than is reasonable given our operating environments. Contractors are absolutely without recourse in most cases. That being said, this is also the case with much current commercial software, but the expectation among many clients is that commercial software is often more developed, proven and vetted than much open source, although that generalization may not be the case with all software.

Another concern contractors have is that their warranty to software may be inadvertently and unintentionally applied to the open source software. In other words, their corporate software warranty may inadvertently encompass open source software. Some open source licenses also prohibit use of the software in "hazardous activities" such as weapon systems.

3. To what extent should the DFARS be revised to specify clearly the rights the Government obtains when a contractor acquires open source software for the Government, and why?

With respect to license restrictions, the different versions of the GNU General Public Licenses issued by the Free Software Foundation (FSF) impose numerous requirements which are difficult to meet in a Government contracts environment without the Government's understanding and approval of these requirements.

Terms that are inconsistent with most open source licenses, but which have been imposed by the Government in Government acquisitions involving commercial computer software are: (1) a requirement that a license be irrevocable; (2) a requirement that a license cannot be terminated for breach; (3) a requirement that the license's warranty, liability and intellectual property infringement disclaimers be deleted or modified, or replaced with clauses such as DFARS 252.246-7001 ("Warranty of data"); (4) a requirement that any licensee indemnification requirements be deleted; (5) a requirement that the license's governing law be modified from state law to the law of federal contracts; (6) a requirement that the software be marked in a way that is inconsistent with the license requirements; (7) a requirement that the license's terms not be applicable to the Government's sublicenses to Government contractors; (8) a requirement that the software be subject to the DFARS clauses applicable to non-commercial computer software; (9) a requirement that the software be subject to the DFARS clauses applicable to commercial technical data such as DFARS 252.227-7015; and (10) a requirement to delete all severability clauses.

Open source software is one form of commercial computer software. Others take the view that open source software is not necessarily "commercial." Currently, the DFARS specifies that the Government's rights in commercial computer software will be the same as those rights granted to the general public in accordance with the licensor's standard commercial license, unless such license does not meet the Government's needs. If the standard commercial license does not meet the Government's needs, the Government is directed to negotiate a license that does. Thus, under the current DFARS regulations, the Government should acquire the open source software in accordance with the terms of the applicable open source license, e.g. the Apache license, the BSD license, the GNU General Public License, etc.

One issue with this approach is that the contractor has virtually no ability to modify the terms of the open source licenses, and thus, may not be able to meet the Government's needs using such open source software, even though that software might be the best solution to the technical requirements. For example, if the Government indicates that a license must be irrevocable, and cannot be terminated, it is not possible to modify the terms of the open source license to meet those requirements. In that case, unless the contractor otherwise obtains the Government's approval to use such code under the applicable license terms, the contractor may need to use different software even if that is not the most efficient way to develop the code in question.

In light of this, it may be helpful to amend the regulations to establish some mechanism for the contractor to provide listings of the open source code that it may or will deliver, the licenses that govern the use of such software, and some statement of the impact on the program if the use of such software is not approved by the Government. Upon receipt of this information, the Government should be directed either: (1) to approve such use in accordance with the terms of the standard open source license; (2) to provide it authorization and consent to infringe the copyright in such software if the Government determines that it cannot comply with the open source license but believes that such use is an acceptable way to meet the Government's needs; or (3) to disapprove the use of such open source software. If such disapproval occurs during contract performance, the regulations should also include a mechanism for recognizing the costs and/or schedule impact that the contractor may experience due to such disapproval. The regulations should also provide a flexible mechanism for updating such listings given that the software development process invariably involves changes in what specific code is used.

To date, we have seen attempts to implement portions of such a process under certain Government solicitations, and under the pending proposed DFARS regulations that re-write DFARS Part 227. The proposed regulations have modified the data rights assertion requirements to require assertions for commercial computer software, and have added a requirement to provide the commercial licenses under which commercial computer software would be licensed to the Government. Such regulations could provide the mechanism for obtaining the necessary information, and perhaps should be modified to add a requirement for the Government to approve or disapprove the use of the open source software terms, including the option for the Contracting Officer to accept the open source license's terms.

Another concern is lumping open source software with other types of commercial software. Even if an existing open source program meets the definition of "commercial item," modifications made to meet contract requirements may result in the modified version no longer meeting that definition. Further, no other commercial software has a feature whereby it can make a Contractor's proprietary code non-proprietary. This "copyleft" issue (i.e., FSF attempts to force the publication of proprietary code that is linked inappropriately to or which modifies GPL code) is not reflected in these questions, but should be raised for discussion at the public forum. Additionally, "copyleft" may force Contractors and the Government, into choosing between compliance with the open source license (e.g., must disclose distributed modifications) or compliance with export regulations (can't disclose "technical data" w/o a license).

We have seen the Government object to certain open source licenses on the basis that license provisions violate the Antideficiency Act (ADA). In such a case, there is a perceived conflict between the Antideficiency Act and the policy to promote the use of open source in the Department of Defense. One example is the Apache 2.0 open source license, which according to Wikipedia covers over 6000 open source projects located on the Sourceforge.net repository. See http://en.wikipedia.org/wiki/Apache_License. This license also covers the Apache Web Server, which is a popular operating environment for hosting websites. The Government's objection to the Apache license is based on paragraph 9, which provides that the licensee indemnifies the developer in certain circumstances. The Principles of Federal Appropriations Law, Third Edition, Volume II at 6-59 to 6-93 discusses indemnification agreements and the ADA in detail and concludes:

"The problem is that [indemnification agreements] create a risk that the government, at some point in the future, may have to pay amounts in excess of available funds. Consequently, with one very limited exception discussed below, GAO and numerous courts have adhered to the rule that, absent express statutory authority, the government may not enter into an agreement to indemnify where the amount of the government's liability is indefinite, indeterminate, or potentially unlimited. Such an agreement would violate the Antideficiency Act, 31 U.S.C. § 1341, and the Adequacy of Appropriations Act, 41 U.S.C. § 11, since it can never be said that sufficient funds have been appropriated to cover the government's indemnification exposure." Principle of Federal Appropriations Law, Third Edition, Volume II, p. 6-59 to 6-60.

Making the indemnity capped or subject to available funds is not possible without negotiating with the author, which defeats in part the purpose of open source software -- to make software free and easy to use. We posit that the indemnification provision in, for example, the Apache license at Section 9 is not in conflict with the Antideficiency Act since the Apache license does not require anyone to indemnify each "Contributor." Indemnification of each "Contributor" is only required if a downstream distributor "chooses to offer...warranty, indemnity or other liability obligations." Only in those circumstances (e.g., Government distributes the software to a third party and chooses to indemnify the third party) must the Government indemnify, defend and hold harmless each Contributor from any liability or claims asserted "by reason of your accepting any such warranty or additional liability."

Other provisions to which the Government has objected include attorneys fees provisions, which provide that the losing party pays the prevailing party's attorneys fees and choice of law provisions that specify forums in which the government may not be sued.

Without guidance on what popular open source licenses are acceptable to the Government generally, the contractor presently takes a risk that the open source software incorporated in government deliverables may not be acceptable to the government.

While it is possible to gain the Government's agreement to certain licenses prior to commencing development, this may not be possible when contractors reuse software provided by the Government as Government Furnished Information (GFI) which contains embedded open source software.

4. Other Inputs.

Security and Information Assurance issues were not addressed by DoD in the questions above. Who will bear the risk that some piece of open source software has malicious code that either makes a product malfunction or covertly releases secret information (commercial or governmental) due to its integration in a secure or secret product or program? Certain licenses such as the GPL and LGPL provide that a licensee redistributing the open source library may not impose further restrictions on the recipient. For example, the LGPL 2.1 license provides: "You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License."

There is a question as to whether or not the imposition of export control restrictions is a "further restriction" on the recipient or merely a covenant to "obey the law." This affects contractors selling to government recipients as well as non-governmental recipients

Also, regarding security, Contractors have the following questions:

- Will the DoD CIO/IA community be represented at the meeting?
- What are the statutory, regulatory and other contractual requirements applicable to the certification and accreditation of DoD systems/IA-enabled systems which incorporate open source software?
- Is DoD planning to establish one consolidated process for both the contractual/legal and technical approvals required to use OSS in DoD systems?
- Is DoD planning to maintain a list of evaluated/certified OSS products, similar to the list maintained by Common Criteria? Will the list be made available to DoD contractors?