

**Defense Information Systems Agency**  
**Suite 3W04 - DISA Code: APC**  
**5275 Leesburg Pike**  
**Falls Church, VA 22041**  
**Attention: DOD Open Source FAQ Comments**  
[PublicAF@ncr.disa.mil](mailto:PublicAF@ncr.disa.mil)

**COMMENTS OF**  
**THE INITIATIVE FOR SOFTWARE CHOICE**  
**REGARDING MITRE'S "USE OF FREE AND OPEN-SOURCE SOFTWARE (FOSS) IN THE**  
**U.S. DEPARTMENT OF DEFENSE" / OPEN SOURCE FAQ COMMENTS**

**Introduction**

The Initiative for Software Choice (ISC, [www.softwarechoice.org](http://www.softwarechoice.org)) – a global coalition of companies and associations dedicated to the principle that governments should procure software products on their merits rather than on the basis of categorical preferences – would like to thank the Defense Information Systems Agency (DISA) for the opportunity to address the MITRE background report,<sup>1</sup> “Use of Free and Open Source Software in the U.S. Department of Defense,” Version 1.2.02, released November 6, 2002 (“Study”).

As touched upon above, the ISC’s main goal is to educate policymakers about the need to remain neutral with respect to government purchase of software. Across the globe, more than two-dozen countries have proposed nearly 70 “preference” proposals (including examples here in the US<sup>2</sup>), many of which seek to automatically create a preference for open source software (OSS) over equally viable hybrid or proprietary offerings. These policies strip customer choice from the selection process, greatly harming the software industry as a whole.

Inarguably, software innovation has been a driving force for economic, social, and technological progress. In fact, it has been the strongest example of successful innovation driven by consumer demand. Allowing multiple software development, business, and licensing models to compete on their merits is the best way to promote software innovation, and to ensure that customers – both public and private – have a broad range of choices in their software purchasing decisions.

As will be elucidated further below, the ISC does not believe that the DoD should openly promote the use of OSS because in each instance, the DoD should choose the software that best meets its needs and acquisition requirements for the particular environment in which the software will be used. The ISC also believes that the DoD’s evaluation of the security aspects of individual software should not be fettered by a preconception that

---

<sup>1</sup> This paper primarily seeks to comment on the Study, which frames a significant portion of the FAQ’s foundation.

<sup>2</sup> For example, as proposed in: S. 2048, the "[Consumer Broadband and Digital Television Promotion Act](#)", introduced in the U.S. Senate on March 21, 2002; and the "[Digital Software Security Act](#)", as drafted for introduction in the California State Assembly in August, 2002.

OSS software is somehow inherently more secure. In addition, the DoD should be free to transfer the results of its R&D available to all interested participants in the marketplace.

### **Study's Hypothetical – To Ban Or Not To Ban – Not Based On Reality**

The Study's framework has been designed around the hypothetical question, "[W]hat would happen if FOSS (which the Study defines as "Free and Open Source Software") software were banned in the DoD?" Having asked that question, the Study concludes "banning FOSS would have immediate, broad, and strongly negative impacts on the ability of many sensitive and security-focused DoD groups to defend against cyberattacks."

The ISC believes that, as a threshold matter, this hypothetical asks the wrong question, because to our knowledge no one seriously seeks a ban on FOSS at the DoD. Each software development model – i.e., OSS, hybrid and proprietary – provides its own mix of benefits to the industry, government and taxpayers. No one benefits when otherwise viable software options are completely removed from competition and evaluation by procurement officials.

Perhaps more troubling, however, is the framing of the hypothetical itself, which suggests a certain mutual exclusivity not mirrored in the software industry. The hypothetical perpetuates the "either-or" supposition being advanced by the marketers of OSS products and services that OSS and proprietary products cannot – or rather, should not – operate together, in heterogeneous environments.

Though the viral nature of some OSS licenses, such as the GNU General Public License (GPL), remains a point of concern for many in the industry (even the Study cautions against accidentally invoking the GPL), it is clear that all models can "get along."

The ISC believes that painting the hypothetical in such stark terms serves only to divide communities that, on their own, already co-exist. Together, the entire industry has benefited and evolved through vigorous, hyperactive competition. Doubtless, banning OSS in any area of the DoD (or elsewhere) would have detrimental repercussions, but such a ban is an egregious straw man that has no anchor in reality. The more relevant and interesting issue is whether the DoD is making software procurement decisions based on appropriate guidelines that are uniformly applied to the full range of software products that their proponents seek to introduce into the DoD.

In this connection, the Study would have been more instructive had it looked at the use of OSS at the DoD, and elucidated whether, in each instance, each OSS application was selected based on application of the same procurement requirements and policies that are consistently applied to proprietary software products. The ISC hopes – but can only assume – that this was the case in each of the 115 applications, and 251 identified uses. Lacking this information, however, the Study contributes little insight and should be

viewed simply as a partial study and/or inventory of OSS uses at the DoD.<sup>3</sup>

### **“Ambiguous Status” & “Limbo Status” Does Not Justify New Policy**

After looking at the uses and benefits of OSS at the DoD, the Study settles on three policy recommendations, which call for:

- Creation of a “generally recognized as safe” FOSS list;
- Development of generic, infrastructure, development, security and research policies; and
- Encouraged use of FOSS to promote product diversity.

While marketers of OSS products would certainly cheer the leg-up over other types of products, the presumably debilitating effects of “ambiguous status” concerns, as well as other OSS apprehensions<sup>4</sup> noted within the Study cannot justify preferential policies in a fully functional, working software market.

The author’s own words reveal just how prevalent OSS is at the DoD, working directly against his conclusions and proposals. The Study notes nearly 115 applications/251 uses of OSS at the DoD. Further, the author surmises that OSS use at the DoD goes well beyond what the informal study had been able to derive.<sup>5</sup> With little exception, the Study’s author trumpets the benefits of the OSS development model,<sup>6</sup> taking liberal occasion to herald the model by noting (among many instances):

- The “*early and rapid closure of security holes...[that] allows rapid response to new or innovative forms of cyberattack, [which] is intrinsic to the FOSS approach and generally impractical in closed source products*”;
- The “*gaming psychology [that] tends to produce an ‘arms race’ mentality,*” which constantly improves OSS security products;
- The “*dominance*” of certain widely-used OSS applications, making some of them virtually peerless in their fields;

---

<sup>3</sup> In fact, at page 11, the author notes that the purpose of the Study was “*to develop as complete a listing of FOSS applications used in the DoD as possible, and to collect representative examples of how those applications are being used.*” Given this stated purpose, the report should be limited to providing the listing and review of how some such applications were used in the DoD. To the extent that the report goes beyond this activity, and offers recommendations that are both unsupported and unwarranted, it should be disregarded by DISA.

<sup>4</sup> See page 3: “*...the combination of an ambiguous status and largely ungrounded fears that it cannot be used with other types of software are keeping FOSS from reaching optimal levels of use*”; and at page 22, “*At present, FOSS is neither approved nor disapproved in most parts of the DoD. This limbo status makes program, project, and developer decisions regarding FOSS difficult. Developers are often aware of the benefits of FOSS products for certain types of applications, but are unwilling to share that knowledge with their supervisors or commanding officers for fear that they will be told that they are using ‘unapproved’ applications.*”

<sup>5</sup> For example, at page 16: “*...the examples clearly represent only the tip of an iceberg in terms the total number of facilities, operators, developers, researchers, and contractors using FOSS applications to support DoD work.*”

<sup>6</sup> The Study’s overall objectivity has been greatly undermined by its lack of dissenting voices, as well as by the fact that MITRE has direct financial interests in the success of the OSS model at the DoD and elsewhere.

- The presumed fact that Internet use at the DoD could hardly occur but for the “*largely FOSS approach, with many of its most mature and widely used components being FOSS*”; and
- The belief that some FOSS languages have become “*so endemic in software development*” projects that banning FOSS would bring several DoD projects to a screeching halt.

To be sure, the OSS model can produce good products. The industry recognizes this, too. Some companies that have largely offered proprietary software in the past – such as IBM, Apple, and Sun – have begun producing products that employ OSS features and architecture, while also continuing to offer proprietary software. Additionally, some commercial software companies have incorporated non-viral open source code (i.e., code not subject to the GPL or similar licenses) into their proprietary systems.

Similarly, the commercial model is attractive to OSS-based companies that seek to enhance their revenues. In fact, some companies that formerly developed software only under an OSS model are beginning to offer alternative, modified proprietary versions, or to rely on intellectual property protection, such as trademark law, to prevent dissipation of the value of their products.

Within this evolutionary context, as lines among formerly separated communities blur, and competitive choices proliferate for individual, commercial, and government customers – why does the DoD need a “promotional” policy to push OSS’ further use?

The answer is – it doesn’t.

Case-by-case choice, driven by the needs of each project, demands the full panoply of solution options. The DoD should reaffirm this long-held policy, which enables developers of software from a variety of business models to compete for DoD business on the basis of which solution best satisfies the DoD’s needs and acquisition objectives for a particular software application.

### **The Security “Non-Debate”**

Over the past couple of years, a debate has emerged concerning what types of software development models enable more secure software products. Statements within the Study<sup>7</sup> apparently attempt to lend credence to the argument that OSS products are somehow more secure than proprietary offerings. These statements, as well as a steady stream of other ephemera from OSS marketers, have been widely used to propound the so-called “fact” that OSS is more secure than that of proprietary/commercial offerings.

As with proprietary offerings, the ISC does not doubt that OSS products can achieve a high level of security. But, that’s about all that can be said with any great accuracy. Although a plethora of studies exists which ask whether OSS is more secure than proprietary software, no unequivocal findings of fact can point to any clear-cut

---

<sup>7</sup> Such as page 2: “*One unexpected result [of the Study] was the degree to which Security depends on FOSS.*”

advantages that software produced under one model has over software produced under the other model.<sup>8</sup> In other words, no single development mode inherently produces safer, more secure software. Further, no software or system based on software – regardless of how it gets produced or built – remains immune from cyberattack.

A development model is only a process. It does not guarantee, in and of itself, that a product produced under that model will be any better than another product produced under a different model. Knowing this, the ISC remains agnostic about the supposed security (or other) benefits that each development model brings. The debate cannot be determined in the abstract – actual results, not process, matters most.

To that end, the ISC would like to reiterate that the touchstone when choosing software must always be merit-based choice. In the context of security, can a software product, faced with the challenges of each unique project, provide the security needed for that unique project? Anything less would severely compromise that project’s efficacy, security or otherwise.

General policy statements that raise one software characteristic over all others regardless of project or departmental needs usurp the needed latitude of government procurement officers to make the best choice for a given endeavor.

Should the DoD or DISA as a whole choose to exclusively promote OSS as the more “secure” platform, such a position would not only represent a momentous shift away from long-held U.S. procurement policy, it would also potentially foreclose the largely proprietary-based IT industry from billions of dollars in federal marketplace business. In doing so, government agencies would be equally disadvantaged, being denied access to the software innovations created by commercial software companies, shut out as a result of these preferential policies. Moreover, both because such policies limit competition and require that additional dollars be spent to acquire software that met policy standards and the needs of the end-user, the overall cost to the taxpayer could increase as well.

### **GPL – Be Careful When Using; Questions Where Federal R&D Involved**

The Study goes to great length educating its readers on what OSS is, although, perhaps intentionally, it glosses over the differences between the GPL and non-viral OSS licenses. At several points within the Study, though, the author does caution that code development under either the OSS model, or specifically with the GPL, “should not be made accidentally.”<sup>9</sup> This is so, explains the author, because integrating non-GPL code

---

<sup>8</sup> At least one report, however, based on data from Carnegie Mellon University’s Computer Emergency Response Team (CERT), suggests that OSS-based Linux faces more security problems than previously acknowledged, running contrary to the popular belief that OSS development inherently leads to more secure products (see ["Study: Linux' Security Problems Outstrip Microsoft's."](#) NewsFactor Network, November 15, 2002, by James Maguire).

<sup>9</sup> For example, see page 19, where the Study notes that basic code developers should take care that any libraries they use “do not use licenses (e.g., the GPL) that would inadvertently require the new software to be FOSS also”; and directly below this reference, where the author notes that “While it may be worth ...[developing code] under a FOSS model, such decisions should not be made accidentally, but should be decided ahead of time.”

with GPL code – the latter being based on “transitive user rights” – means that any “new [or derived] work must also be placed under the GPL.”

For proprietary and/or hybrid companies, such a concept runs contrary to their business model. Companies expend significant resources walling off their proprietary intellectual property (IP) and associated software development from an inadvertent integration with code that is subject to the GPL. When products become integrated with GPL software, the rights, benefits and incentives of the subsumed non-GPL IP are lost.

While the law on this matter remains untested, it makes sense for companies to be highly risk averse in this area, striking a more defensive posture when confronted with software development that may implicate GPL code or similar coding environments.<sup>10</sup> Commercial and hybrid software developers generally do not want to risk losing their investment because of “transitive user rights.”

The ISC believes that developers should be free to pick the model of their choosing. To be sure, plenty of less-restrictive OSS licenses exist (such as the Berkeley Software Distribution license) that could achieve many of the same communal benefits espoused by proponents of the GPL, but with few, if any, negative effects on subsequent commercialization. However, if a developer wants to build his/her product under the GPL, so be it – it’s their choice, and the resulting product will be part of the software community competing for customer attention and business.

However, where government-funded R&D is involved, application of the restrictive GPL takes on an altogether different meaning. The Study notes that over 50 percent of the DoD’s OSS products are GPL-based. Thus, because of the GPL’s “transitive user rights,” at least half of the DoD’s OSS efforts, were they to be more widely disseminated, would largely foreclose proprietary and/or hybrid companies from further developing the software and commercializing the results. The same is true for any outside R&D funded by the DoD – if it is GPL-based, proprietary companies cannot directly benefit from it.

Limiting those who would otherwise participate from coming to the table reduces the ultimate usefulness of any software solution developed through federal R&D. Current U.S. policy – as seen in the Bayh-Dole Act – advances government R&D by enabling universities, small businesses and others that participate in federal R&D programs to retain title to their subsequent results. Promoting the public availability of federally funded R&D inventions through commercialization has served America well; it has helped broaden the dissemination of R&D that might otherwise sit dormant and un-exploited. This elective policy remains sound, and does not warrant being changed, especially in light of America’s need for enhanced security, post 9-11.

### **Leave “Promotional” Policies To The Marketers, Not To Government Officials**

As the author of the Study has amply demonstrated, the DoD has not hesitated to adopt OSS software, despite the ostensible “ambiguous status,” “limbo status” or operational

---

<sup>10</sup> The limited application of the Microsoft/MIT EULA is a case in point, being designed to minimize and/or thwart the third-party “GPL-ization” of intellectual property, whether intentional or not, during the beta process.

apprehensions over OSS. The government should not be in the business of categorical preferences or “promotions” when the usual processes of competing for government business on the merits are available and effective. Accordingly, the ISC respectfully urges that the DoD/DISA avoid crafting needless and potentially detrimental IT policy to promote the use of OSS at the DoD.

Sincerely,

A handwritten signature in black ink, appearing to read 'Bob Kramer', with a long horizontal line extending to the right.

Bob Kramer  
Executive Director – Initiative for Software Choice  
4350 N. Fairfax Dr.  
Suite 440  
Arlington, VA 22203  
(ph) 703-812-1333  
(fax) 703-812-1337

November 26, 2002