What Should Governments Examine in Acquiring COTS Open Source Software (OSS)?

David A. Wheeler
Institute for Defense Analyses
February 2, 2004

This presentation contains the views of the author and does not indicate endorsement by IDA, the U.S. government, or the U.S. Department of Defense. Copies available at http://www.dwheeler.com/government_oss.pdf

Outline

- **Same (OSS vs. Proprietary)**
- **Different (OSS vs. Proprietary)**
- **OSS Challenges**
- **Closing Remarks**

Same (OSS vs. Proprietary)

- **Negotiate best options with all parties, *then* select**
  - Good: Israeli government's process
  - Unwise: Media reports of Newham Borough Council's
- **Evaluation criteria**
  - Functionality, cost, market share, support, maintenance/longevity, reliability, performance, scalability, flexibility, legal/license (inc. *rights and responsibilities*), other

  > OSS gives rights to view, modify, and redistribute

- **Warranty & indemnification**
  - Disclaimed by *both* proprietary & OSS licenses (generally)
  - Indemnification exception: Linux (OSDL, HP, RH, Novell)
- **Developer trustworthiness usually unknown**
  - Can review OSS code & sometimes proprietary

Different (OSS vs. Proprietary)

- **Process&code openness means more&different sources of evaluation information**
  - Bug databases, mailing list discussions, …
  - Anyone can review/comment on design
  - Anyone (inc. you) can evaluate source code for security
  - See http: //www.dwheeler.com/oss_fs_eval.html
- **Proprietary=pay/use, OSS=pay/improvement**
  - In either case pay for installation, training, support
  - In OSS, pay can be time and/or money
- **Support can be competed & changed**
  - OSS vendors, government support contracts, self
- **OSS can be modified & redistributed**
  - New option, but need to know when to modify
  - Forking usually fails; generally work with community

OSS Challenges

1. **Ensuring OSS considered in acquisitions**
   - **Acquisition processes developed before OSS rise**
   - **Many OSS projects don't respond to solicitations&RFPs**
2. **Ensuring license compliance**
   - **No *use* requirements. Education needed on redistributing copyleft (but easier than proprietary)**
3. **CC security evaluations (no funding model)**
   - **Government-funded evaluation for free use/support?**
4. **Support if there's no traditional vendor**
5. **Dependence on proprietary formats/protocols**
   - **Use open standards. DoD JTA (DISR) wants: mature, not proprietary, publicly held, multi-vendor commercial support, international>national, *don't require patents*, …**
   - **Government policy issue: software patents justified?**

Closing Remarks

- **OSS options should always be considered**
- **OSS can be very flexible & often lower costs**
  - **Directly and as competition**
- **Need to understand differences to apply OSS**
- **OSS raises strategic questions for governments**
  - **Level-playing-field (e.g., U.S. DoD)**
  - **Other: Industrial policy (encourage local services & research), counter dependency on external entity, transparency in government, longevity of records, …**
- **Need creativity**
  - **Risk mitigation, not risk avoidance**
  - **Hybrid OSS/proprietary, paying for OSS improvements, or starting OSS project (esp. in research or standards-setting) *might* be the best option in your case**

Acronyms

- **COTS: Commercial Off-the-Shelf (either proprietary or OSS)**
- **DoD: Department of Defense**
- **HP: Hewlitt-Packard Corporation**
- **JTA: Joint Technical Architecture (list of standards for the DoD); being renamed to DISR**
- **OSDL: Open Source Development Labs**
- **OSS: Open Source Software**
- **RFP: Request for Proposal**
- **RH: Red Hat, Inc.**
- **U.S.: United States**

Trademarks belong to the trademark holder.

Interesting Documents/Sites

- "Why OSS/FS? Look at the Numbers!" http://www.dwheeler.com/oss_fs_why.html
- "Use of Free and Open Source Software in the US Dept. of Defense" (MITRE, sponsored by DISA)
- President's Information Technology Advisory Committee (PITAC) -- Panel on Open Source Software for High End Computing, October 2000
- "Open Source Software (OSS) in the DoD," DoD memo signed by John P. Stenbit (DoD CIO), May 28, 2003
- Center of Open Source and Government (EgovOS) http://www.egovos.org/
- OpenSector.org http://opensector.org
- Open Source and Industry Alliance http://www.osaia.org
- Open Source Initiative http://www.opensource.org
- Free Software Foundation http://www.fsf.org
- OSS/FS References http://www.dwheeler.com/oss_fs_refs.html