What is Open Source Software?

Andy Murren
Sila Solutions Group
amurren@silasg.com

4 Oct 2016

What is Open Source Software (OSS)?

Open Source Software is *COMMERCIAL*[*] software!

- "software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software." - DoD
- Originally known as “Free Software” referring to liberty not cost
- Also know as: Libre Software, Free-Libre Software, Free/Open Source Software (FOSS), Free-Libre /Open Source Software (FLOSS)

** Per OMB and DoD rules OSS is almost always COTS. There are a few special cases where OSS is not COTS. Consult your legal team for specific guidance.*

The Open Source Definition (OSD) Criteria

1. Free Redistribution
2. Source Code
3. Derived Works
4. Integrity of The Author's Source Code
5. No Discrimination Against Persons or Groups
6. No Discrimination Against Fields of Endeavor
7. Distribution of License
8. License Must Not Be Specific to a Product
9. License Must Not Restrict Other Software
10. License Must Be Technology-Neutral

What OSS is Not

- An insidious Communist plot to destroy capitalism
- Substantially more or less secure than proprietary software
- A magic bullet to solve every problem, which may be proprietary, Open Core, OSS, or a combination
- Without cost
- Without the same need to manage and update as proprietary software
- The same as Shareware or Freeware, which are proprietary

Why to Use OSS

- Reduced Costs
  - Total Cost of Ownership (TCO)
  - Development costs
  - Support costs
  - No per user/per instance costs
- Interoperability using open standards and APIs
- Can evaluate for suitability, security, etc.
- Can modify to address user’s needs
- Avoid vendor or integrator lock-in
- Ability to do rapid prototyping/proof of concept
- Can share and redistribute with other organizations

OSS is COTS

Why Not to Use OSS

- Software does not provide required functionality
- License compliance considerations
- Insufficient external support available
- Incompatibilities with existing systems or software
- Lack of required skills in the organization
- Missing features (e.g. support for FIPS approved encryption)

Legal Status of OSS for Government Use

- OSS meets the definition of Commercial software (COTS) under the FAR and DFAR
- It can be used by Federal agencies the same as other COTS
- Must comply with the software's license
- Contribution of modifications to back to the developer community encouraged

OSS is COTS

Types of OSS licenses

- Copyright law: Must have permission to copy software
  - Permission is given by a license
  - Proprietary software: Pay for a license to use a copy/copies
  - OSS licenses grant more rights, but still conditional licenses
- Can be grouped into three categories (differing goals):
  - Permissive: Can make proprietary versions (MIT, BSD-new)
  - Strongly protective: Can't distribute proprietary version or combined (linked) into proprietary work; if give someone the binary, must give them the source if asked (GPL)
  - Weakly protective: Can't distribute proprietary version of this component, but can link into larger proprietary work (LGPL)
- The most popular OSS licenses tend to be compatible
  - Compatible = you can create larger programs by combining software with different licenses (must obey all of them)

Source: Dr. D. Wheeler "Open Source Software (OSS or FLOSS), Government, and Cyber Security" 2013

Dual Licenses

- Software is licensed under one OSS license and either an OSS license or a Proprietary license
- OSS/OSS license scheme
  - Allows users to select how to use the software and license derived works
  - Example: Perl programming language licensed under Perl Artistic License and GNU General Public License (GPL)
- OSS/Proprietary license scheme
  - Allows companies to distribute software as OSS and sell software proprietary licenses
  - Sometimes referred to as Open Core
  - Example: SonarSource Community Edition licensed under GNU Lesser General Public License (LGPL), other versions available under proprietary license

Open Core

- A hybrid of Open Source and Proprietary software
- Core functionality available under an OSS license
- Enhanced features and functionality available under Proprietary license
- Using enhanced features and functionality may result in vendor lock-in
- Under some licensing schemes user changes or enhancements may become proprietary vendor property

Types and Classes of Software

Types

- Closed Source
  - Proprietary
  - Shareware
  - Freeware
- Open Source
  - Commercially Supported
  - Foundation Supported
  - Community Supported

Classes

- *Applications:* Off-the-shelf products that are complete and that can be run without any additional development
- *Components:* Software that cannot be run without additional development or integration, such as libraries or frameworks

OSS is COTS

Open Source Software Support

	Commercial	Community	
		Foundation	Independent
Bug Fixes	Yes	Yes	Yes
Call Center Support	Yes	No	No
Chat or IM	Some	Some	Some
Consulting Services	Some	Some	No
Documentation	Yes	Yes	Yes
Email Support	Yes	Yes	Yes
Feature Updates	Yes	Yes	Yes
On-line Forums	Yes	Yes	Yes
Security Patches	Yes	Yes	Yes
SLA	Some	No	No

Note: The Open Source components of Open Core are generally supported similar to Foundation and the proprietary components the same as closed source proprietary software.

Examples of OSS and It’s Primary Support

- Hadoop Software Library – The Apache Foundation
- LibreOffice – The Document Foundation
- Linux Operating System
  - Red Hat Enterprise Linux – Red Hat Corporation
  - CentOS - Community
- SonarSource Code Quality Management Tool
  - SonarSource Community Edition – Community
  - SonarSource Professional Edition – SonarSource
- Struts Java Framework – The Apache Foundation

Comparison of Proprietary SW & OSS

	Closed Source				Open Core	Open Source	
	Proprietary	Shareware	Freeware	Private	Proprietary Components	Commercial Support	Community Support
Source Code Available	No or only with restrictions	No	No	No or only with restrictions	No or only with restrictions	Yes	Yes
Binary Executables Available	Yes	Yes	Yes	Yes	Yes	Yes	Usually
No Restrictions on How Used	No	No	No	No	No	Yes	Yes
Unlimited Number of Users	No	No	No	No or only with restrictions	No or only with restrictions	Yes	Yes
Right to Study How Software Works	No	No	No	No or only with restrictions	No	Yes	Yes
Right to Redistribute	No	No	Yes	No	No	Yes	Yes
Right to Modify	No	No	No	No or only with restrictions	No or only with restrictions	Yes	Yes
Right to Fork	No	No	No	No	No	Usually	Usually

OSS is COTS

Classes of Software - Applications

Application	Examples	Commercially Supported	Community Supported
Operating System	Red Hat Enterprise Linux	X	X
	CentOS Linux		X
Web Server	Apache	X*	X
	NGINX	X	X
Productivity Suite	LibreOffice	X*	X
Database Servers	PostgreSQL	X*	X
	Accumulo	X*	X

Many organizations are already using OSS for infrastructure operations (such as DNS and NTP services) along side proprietary software. Open Source applications can often provide equivalent functionality to proprietary or internally developed software for other activities and operations at reduced costs.

* Commercial support available via third party

OSS is COTS

Classes of Software - Components

Application	Examples	Commercially Supported	Community Supported
Encryption	OpenSSL GnuTLS	X X*	X X
Development Frameworks	Struts Django	X*	X X
Development Libraries	glibc C library XMLBeans		X X

OSS is pervasive in proprietary products. The HeartBleed vulnerability of 2014 in OpenSSL impacted products from Cisco, HP, IBM, Intel, Nokia, and Oracle. OEMs and integrators are using OSS extensively. Frequently internal developers use OSS without management realizing it.

* Commercial support available via third party

Managing OSS

- Both commercially and community supported OSS applications can be managed using the same policies and processes as commercial proprietary applications
- Commercially supported OSS components can be managed using the same policies and processes as commercial proprietary applications
- Community supported OSS applications and components organizations need to have policies and processes added to replace support normally provided by commercial support
- For OSS included by integrators and developers for custom software the vendor and customer must coordinate responsibility for long term support of the OSS

The Cost of Using OSS

- Using Commercially supported OSS can be more cost effective than using Community supported OSS
- A 2011 study by IDC comparing organizations using RedHat Enterprise Linux (RHEL) to organizations using free Community supported Linux found that using OSS can result in substantial cost savings, but can additional costs are incurred when relying exclusively on internal resources for support.

	RHEL	Free
Servers per administrator	174	97
End users per administrator	422	358
Annual IT labor costs per 100 users	$18,960	$37,099
Annual downtime cost per 100 users	$12	$67
Total operational costs per year per 100 users	$37,494	$62,305

Source: IDC White Paper "Understanding Linux Deployment Strategies: The Business Case for Standardizing on Red Hat Enterprise Linux" 2011

Federal Code Reuse

- Federal CIO Memo M-16-21 “Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software” dated 8 Aug 2016 requires:
  - “rights to Government-wide reuse and rights to modify the code” for custom-developed code
  - “Each agency shall release as OSS at least 20 percent of its new custom-developed code”
  - “Require[s] agencies to consider the value of publishing custom code as OSS”

The Federal Government requires Open Source as part of IT

Summary

- OSS is almost always COTS
- Select the best software/support for the mission, be it proprietary, Open Core, or OSS
- Federal agencies are required to reuse source code internally and where possible to acquire and contribute to OSS
- Management of OSS is not significantly different from managing proprietary software
- Software vendors and integrators use OSS to reduce cost and improve the products they sell to commercial and government clients
- OSS can result in significant cost saving, but beware of hidden costs
- Agencies must get legal guidance to comply with both proprietary and OSS licenses