



Top 10 Questions to Ask Before Exporting Software Containing Encryption

January 14, 2009

Agenda

- Introduction
- FOSSBazaar
- Top Ten Questions – Before Exporting Encryption
- Questions & Answers



Speakers



Eran Strod

- Director of Product Marketing
- Black Duck Software

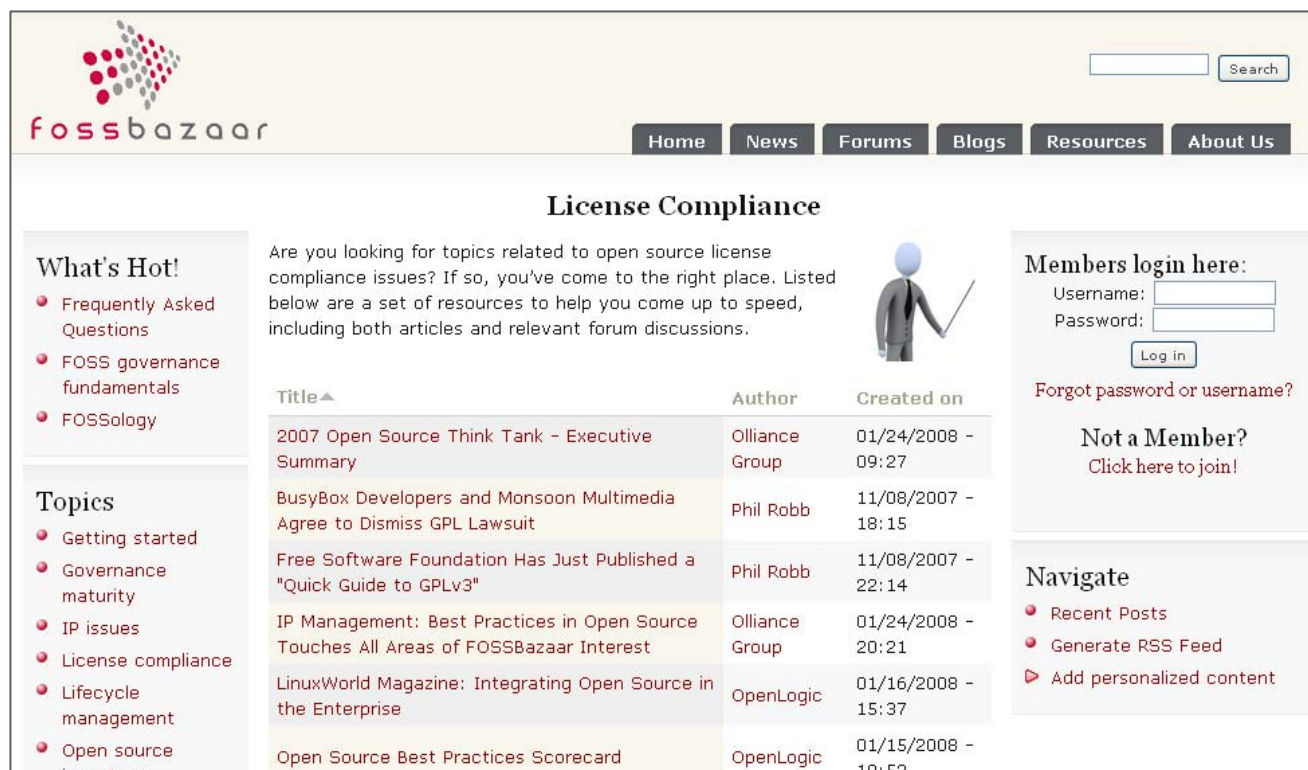


Phil Robb

- General Manager, FOSSBazaar.org
- Director - Open Source Program Office, Hewlett Packard



What is FOSSBazaar?



The screenshot shows the FOSSBazaar website interface. At the top left is the FOSSBazaar logo, and at the top right is a search bar. A navigation menu includes Home, News, Forums, Blogs, Resources, and About Us. The main content area is titled 'License Compliance' and contains an introductory paragraph, a table of articles, and several sidebars.

License Compliance

Are you looking for topics related to open source license compliance issues? If so, you've come to the right place. Listed below are a set of resources to help you come up to speed, including both articles and relevant forum discussions.

Title▲	Author	Created on
2007 Open Source Think Tank - Executive Summary	Olliance Group	01/24/2008 - 09:27
BusyBox Developers and Monsoon Multimedia Agree to Dismiss GPL Lawsuit	Phil Robb	11/08/2007 - 18:15
Free Software Foundation Has Just Published a "Quick Guide to GPLv3"	Phil Robb	11/08/2007 - 22:14
IP Management: Best Practices in Open Source Touches All Areas of FOSSBazaar Interest	Olliance Group	01/24/2008 - 20:21
LinuxWorld Magazine: Integrating Open Source in the Enterprise	OpenLogic	01/16/2008 - 15:37
Open Source Best Practices Scorecard	OpenLogic	01/15/2008 - 19:52

What's Hot!

- Frequently Asked Questions
- FOSS governance fundamentals
- FOSSology

Members login here:

Username:
Password:

Forgot password or username?

Not a Member?
Click here to join!

Topics

- Getting started
- Governance maturity
- IP issues
- License compliance
- Lifecycle management
- Open source

Navigate

- Recent Posts
- Generate RSS Feed
- Add personalized content

A community to develop and share best practices for open source governance in the enterprise

FOSSBazaar is a Working Group of the Linux Foundation

Complex Software Sourcing



- External sources of code
 - Open source
 - Outsourcing
 - Insourcing
 - Undocumented reuse
- Software dependencies
- Dormant code



Mixed Code Risks



Loss of Intellectual Property



License Rights and Restrictions



Software Defects

Export Regulations

Injunctions



Contractual Obligations

Security Vulnerabilities



Escalating Support Costs

Question 1 – Where is the item being exported?

- Wassenaar Arrangement
 - 40-country agreement controlling export of weapons and of dual-use goods (military and civil) like *cryptography*
- United States Controls
 - Under US Department of Commerce
 - Bureau of Industry and Security, (**BIS**)
 - Export Administration Regulations ("**EAR**")
- BIS Key areas of concern:
 - Terrorist supporting and embargoed countries:
 - Cuba, Iran, North Korea, Sudan, Syria
 - Terrorist organizations:
 - Al Qaeda, Hamas, and others
 - Denied Persons List, (DPL):
 - Maintained by the BIS - updated frequently
 - China – specific export restrictions
 - EU+ and Canada are less restricted
- ITAR



Documented Legal Actions

- Northrop Grumman
 - \$400K civil penalty
- FMC Technologies
 - \$610,000 civil penalty
- DHL
 - \$9.4M civil penalty
- LogicaCMG
 - \$50,000 criminal fine
 - \$90,000 administrative penalty
- Neopoint
 - \$95,000 civil penalty
- China May Company
 - Prison sentence
- Technical Integration Group (TIGS)
 - Prison sentence
 - \$1.1M fine
- Realtek Semiconductor
 - \$44,000 penalty
 - Two year denial of export privileges



Defining Export

Common methods

- Shipping / postal mail
- Hand-carried
- Email
- Upload/download to internet site
- Conversation (technology)
- Transmit to foreign nationals in US



Per US Department of Commerce BIS



Question 2 – What is being exported?

- ECCN 5D992
 - Cryptologic equipment, software for the development, production or use of
 - **Not covered by 5D002**
 - Information security equipment, software for the development, production or use of
 - **Not covered by 5D002**
 - *Virus Protection Software (No Longer Covered)*
 - NLR to all but Country Group E

- ECCN 5D002
 - *Information security software (unless decontrolled)*
 - *Encryption Software (unless decontrolled)*
 - License Required to All Countries Except Canada
 - **Unless a License Exception Applies (ENC, TSU, etc.)**



Description	ECCN Citation
Imaging devices	6A002
Imaging device manufacturing equipment and systems	3B991.b Note
Image intensifier tubes & components	6A002.a.2
Image intensifier tubes, direct view	6A002.c.1
Image transfer equipment	3B991.b.2
Imaging cameras	6A003.b
Imaging cameras with focal plane arrays of 6A002a.3	6A003.b.4
Imaging cameras with image intensifiers of 6A002a.2.a	6A003.b.3
Imaging devices	6A203.b.3
Imaging equipment, visible & infrared	6A002.c
Imaging sensors, multispectral and monospectral	6A002.b
Imaging systems, underwater electronic	8A002.f
Immobilization guns and projectiles	0A985
Immunotoxins and vaccines	1C991
Impregnated cathodes for electronic tubes	3A001.b.1.c
Imprint lithography equipment	3B001.f.2
Improvised explosive devices (specially designed or modified disposal equipment , components, and accessories)	1A006
IMU platform balance fixture	7B003, 7B101
IMU platform tester	7B003, 7B101
IMU stable element handling fixture	7B003, 7B101
Incinerators designed to destroy the chemicals controlled by 1C350	2B350.j
Independent (air) power systems underwater	8A002.j
Indicator heads designed/modified for use with balancing machines in 2B119.a	2B119.b
Indium organo-metallic compounds	3C003
Indium III/V compounds substrates	3C001.c
Induction coil magnetometers	6A006.c
Induction furnace, controlled environment inert gas	2B226
Induction furnace, vacuum	2B226
Inductively coupled plasma mass spectrometers (ICP/MS)	3A233.a
Industrial process control hardware/systems designed for power industries	1B999.c
Industrial process control hardware/systems designed for power industries controlled by 1B999, software for	1D999.a
Inert gas environment induction furnaces	2B226
Inertial Measurement Equipment for Azimuth, Heading, or True North determination, and specially designed components therefor	7A003.c
Inertial measurement equipment	7A003
Inertial measurement unit tester (IMU module)	7A003, 7B003, 7B101
Inertial navigation, systems/equipment/components	7A103.a
Inertial navigation, systems/equipment/components	7A003
Inertial navigation systems not controlled by 7A003 or 7A103	7A994
Inertial navigation system software, source code	7D002
Inertial reference Systems (IRS)	7A003.c
Inertial sensors, optical fiber	6A002.d.3.a
Inflatable boats and components	8A992.f

Question 3 – Is the item controlled?

D. SOFTWARE

5D002 “Software” as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, AT, EI

Control(s)

Country Chart

NS applies to entire entry

NS Column 1

AT applies to entire entry

AT Column 1

EI applies to “software” in **5D002**.a or c.1 for

December 11, 2009

Source: BIS Category 5 (Part 2) - Information Security



Copyright © 2010 Black Duck Software, Inc. All Rights Reserved.

Know Your Code.™

Question 4 – Where is it going?

Commerce Control List Overview and the Country Chart

Supplement No. 1 to Part 738—page 1

Commerce Country Chart

Reason for Control

Countries	Chemical & Biological Weapons			Nuclear Nonproliferation		National Security		Missile Tech	Regional Stability		Firearms Convention	Crime Control			Anti-Terrorism	
	CB	CB	CB	NP	NP	NS	NS	MT	RS	RS	FC	CC	CC	CC	AT	AT
	1	2	3	1	2	1	2	1	1	2	1	1	2	3	1	2
Afghanistan	X	X	X	X		X	X	X	X	X		X		X		
Albania ^{2,3}	X	X		X		X	X	X	X							
Algeria	X	X		X		X	X	X	X	X		X		X		
Andorra	X	X		X		X	X	X	X	X		X		X		
Angola	X	X		X		X	X	X	X	X		X		X		
Antigua & Barbuda	X	X		X		X	X	X	X	X	X	X		X		
Argentina	X					X	X	X	X	X	X	X		X		
Armenia	X	X	X	X		X	X	X	X	X		X	X			
Aruba	X	X		X		X	X	X	X	X		X		X		
Australia ³	X					X		X	X							
Austria ^{3,4}	X					X		X	X	X		X		X		
Azerbaijan	X	X	X	X		X	X	X	X	X		X	X			
Bahamas, The	X	X		X		X	X	X	X	X	X	X		X		
Bahrain	X	X	X	X		X	X	X	X	X		X		X		

Source: BIS Supplement No. 1 to Part 738, Commerce Country Chart



Copyright © 2010 Black Duck Software, Inc. All Rights Reserved.

Know Your Code.™

Question 5 – Who will receive the item?

- Commercial enterprise
- Government
- Individual
- Organization

- Denied Person's List

Name
A. ROSENTHAL (PTY) LTD.
A. ROSENTHAL (PTY) LTD.
ACE, IAN
ADT ANALOG AND DIGITAL TECHNIK
AGNESE, ANDREE
AGNESE, HELENE
AGNESE, SABA
AHMAD, TARIQ
AHMED, TARIQ
AHMED, YASMIN
AHUJA, AJAY
AL KAYALI CORPORATION
AL KAYALI, MAYSOON
AL KAYALI, MAYSOON
AL NASSER, ABDULAH
AL NASSER, ABDULAH
AL NASSER, ABDULLAH
ALEX GOH
ALEXANYAN, VLADIMIR
ALL PORTS, INCORPORATED
ALLWAYS, INC.



Question 6 – How will the item be used?

Controlled

- Nuclear, chemical, and biological weapons,
- Related systems
 - Missile delivery systems
 - Certain rocket systems
- Unmanned air vehicles
 - in destinations listed in Part 744 of the regulations.

See License Exceptions...



Question 7 – Does the software have encryption content?

Yes, but...

- Fixed cryptography
 - See if more sensitive CCL restrictions apply
- Limited crypto functionality
 - Access control, authentication except communications
- Decontrolled crypto functionality
- Weak cryptography

5D992 (SW) without BIS notification or review



Question 8 - Is the software publicly available?

- Publicly available software
 - Cost of reproduction or
 - Freely downloadable
- Notification to BIS and NSA
 - <http://www.bis.doc.gov/encryption/pubavailencsourcecodenotify.html>
- Examples
- Commercial use of OSS

Handling Cryptography within an ASF Release

Purpose and Intended Audience

This page provides PMC members with the information they need to ensure U.S. export control laws are satisfied for ASF product distributions that contain or are "specially designed" to use cryptography.

This page is not intended for users of Apache products. Users should consult the [export control status of our products](#).

Overview

The U.S. Government places **restrictions on the export** of some types of software, such as software employing cryptographic functions. Fortunately, the **TSU exception** to these restrictions, EAR 740.13(e), applies to cryptography of concern to the ASF.

PMCs considering including cryptographic functionality within their products or specially designing their products to use other software with cryptographic functionality should take the following steps **before placing such code on any ASF server, including commits to subversion**:

1. **Check the Export Control Classification Number (ECCN).**
2. **Update the Exports Page with Source Links.**
3. **Notify the U.S. Government of the new code.**
4. **Inform users with a crypto notice in the distribution's README and download pages.**

Source: <http://www.apache.org/dev/crypto.html>



Encryption Algorithms in OSS

- 14,000 projects contain encryption

<i>Algorithm</i>	<i>%</i>	<i>Type</i>	<i>Encryption Only</i>
<i>RSA</i>	13%	Asymmetric	
<i>DSA</i>	9%	Signature	*
<i>DES</i>	9%	Symmetric	
<i>MD5</i>	8%	Hash	*
<i>SHA</i>	8%	Hash	*
<i>Blowfish</i>	6%	Symmetric	
<i>Diffie-Hellman</i>	6%	Keyman	
<i>HMAC</i>	5%	Mac	*
<i>ElGamal</i>	5%	Asymmetric	
<i>AES</i>	5%	Symmetric	
<i>Sub Total</i>	74%		
<i>Other</i>	26%		
<i>Total</i>	100%		

- ~ 4,000 require BIS filing
- Over 3,900 projects require review
- OSS projects may use license exception TSU

Source: Black Duck KnowledgeBase, October 2009



Question 9 – How strong is the encryption?

- Weak encryption
 - 56-bit or Less Symmetrical
 - 64-bit or Less Symmetrical and “Mass Market”
 - 512-bit or Less Asymmetrical
 - 112-bit or Less Elliptic Curve
- Semi-strong
 - 80-bit or Less Symmetrical
 - 1024-bit or Less Asymmetrical
 - 160-bit or Less Elliptic Curve
- Strong
 - File for license, review, notification or classification
- Remove crypto?



Question 10 – Can an exception be used?

- Specific functions or “ancillary encryption”
- Foreign products
- US Subsidiary
- “License Free Zone” Companies
- “Mass market”
- Others



Recommended process for compliance

- Written policies / procedures
 - Training and tools
- Bill-of-Materials
 - Code audit
 - Discovery of open source (and other external) software
- Inbound approval process
- Outbound approval process
- BIS notifications/filings
- Record keeping



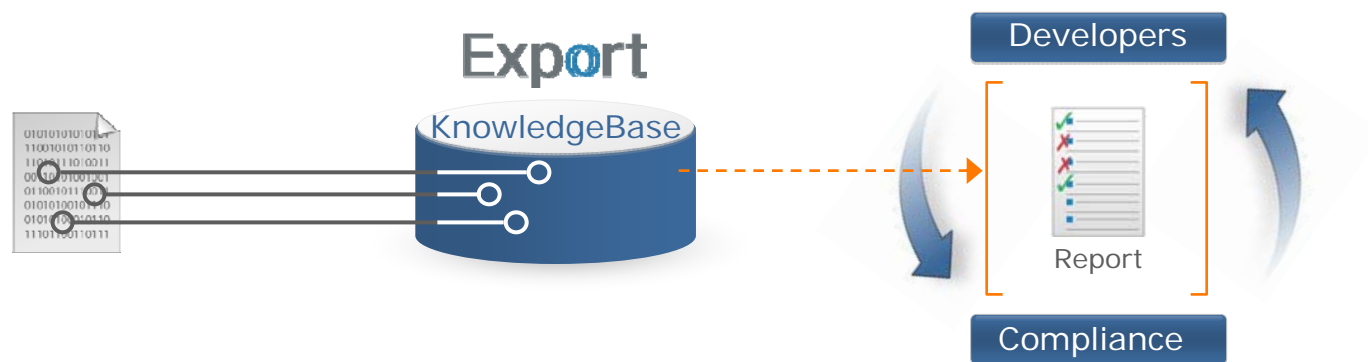


Questions & Answers

Export

Encryption Compliance Management

- Find cryptographic code embedded in complex software
- Improve compliance with export and other government regulations
- Streamline compliance processes



Resources

- Webinar
 - How to Comply with Current U.S. Encryption Export Controls
 - Unlocking Software Export Classifications
 - www.blackducksoftware.com/resources
- White Papers
 - Software Encryption Export Considerations
 - A Guide to Software Encryption Export Compliance
- Black Duck Export Product Page
 - www.blackducksoftware.com/export
- Export and Reexport Compliance Guide
 - Available from Black Duck



Questions and Answers

Please type your question into the chat box
(right side)

- For more information

- **Eran Strod** - estrod@blackducksoftware.com
- To learn more about **Black Duck** Export - Encryption Export Compliance Management:

www.blackducksoftware.com/export

or send email to:

info@blackducksoftware.com

- To follow up with **FossBazaar**:

feedback@fossbazaar.org





Thank You For
Attending

Until next time...