Modules

There are four modules that are being used with Open Source Licenses. These modules are:

- ECOS Operating Sysyem, with GPL license
- FIPS-197, with LGPL license
- FIPS 180-2 SHA-256 hash, PKCS #5 PBKDF1 key derivation and HMAC SHA-256, with MIT-style licenses
- SPI module, with LGPL license

For every block listed above, there should be a separate section in the user manual with the required disclaimers.

Additionally, ECOS and FIPS-197 should also incorporate a procedure on how and from where to retrieve the source codes. You should receive the required source files together with this document.

ECOS OPERATING SYSTEM

Recommendation

The source code of ECOS OS should be made available, and a direction and the mechanism of where and how to retrieve should appear on the user manual. The following is an example of how such an offer could be written:

```
The source code of eCos may be obtained from http://ecos.sourceware.org/ or by
writing to [Your entity name] at [Your entity address] for a small fee to cover
the cost of reproduction
```

A copy of the ECOS OS the way it is used by FW (ecos.tar) should be received by you together with this document.

FIPS-197

Recommendation

The source code of FIPS-197 should be made available, and a direction and the mechanism of where and how to retrieve should appear on the user manual.

The source code of FIPS-97 may be obtained by writing to [Your entity name] at [Your entity address] for a small fee to cover the cost of reproduction

A copy of the relevant source code file (aes.c) should be received by you together with this document.

Disclaimers Text

You should also include the following source disclaimer in the user manual:

```
/*
 *  FIPS-197 compliant AES implementation
 *
 *  Copyright (C) 2003-2006  Christophe Devine
 *
 *  This library is free software; you can redistribute it and/or
 *  modify it under the terms of the GNU Lesser General Public
 *  License, version 2.1 as published by the Free Software Foundation.
 *
 *  This library is distributed in the hope that it will be useful,
 *  but WITHOUT ANY WARRANTY; without even the implied warranty of
 *  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
 *  Lesser General Public License for more details.
 *
 *  You should have received a copy of the GNU Lesser General Public
 *  License along with this library; if not, write to the Free Software
 *  Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston,
 *  MA  02110-1301  USA
 */
/*  The AES block cipher was designed by Vincent Rijmen and Joan Daemen.
 *
 *  http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf
 *  http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
 */
```

FIPS 180-2 SHA-256 hash and PKCS #5 PBKDF1 key derivation and HMAC SHA-256

Recommendation

For the MIT-style licenses (FIPS 180-2 SHA-256 hash and PKCS #5 PBKDF1 key derivation and HMAC SHA-256) you should simply reproduce the source disclaimers in the user manual.

Disclaimers FIPS 1802-2 and SHA-256 hash

The source disclaimer for this function is:

```
/*
 * FIPS 180-2 SHA-224/256/384/512 implementation
 * Last update: 02/02/2007
 * Issue date:  04/30/2005
 *
 * Copyright (C) 2005, 2007 Olivier Gay <olivier.gay@a3.epfl.ch>
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
```

Disclaimers for PKCS #5 PBKDF1 key derivation and HMAC SHA-256

The source disclaimer for this function is:

```
/*---------------------------------------------------------------------------
 Copyright (c) 2002, Dr Brian Gladman, Worcester, UK.   All rights reserved.

 LICENSE TERMS

 The free distribution and use of this software in both source and binary form is
allowed (with or without changes) provided that:

   1. distributions of this source code include the above copyright
      notice, this list of conditions and the following disclaimer;

   2. distributions in binary form include the above copyright
      notice, this list of conditions and the following disclaimer
      in the documentation and/or other associated materials;

   3. the copyright holder's name is not used to endorse products
      built using this software without specific written permission.

 ALTERNATIVELY, provided that this notice is retained in full, this product may
be distributed under the terms of the GNU General Public License (GPL), in which
case the provisions of the GPL apply INSTEAD OF those given above.

 DISCLAIMER

 This software is provided 'as is' with no explicit or implied warranties in
respect of its properties, including, but not limited to, correctness and/or
fitness for purpose.
 ---------------------------------------------------------------------------
 Issue Date: 26/08/2003

 This is an implementation of HMAC, the FIPS standard keyed hash function */
```

SPI

Recommendation

You should simply reproduce the source disclaimers in the user manual.

Disclaimers

The source disclaimer for this function is:

```
//////////////////////////////////////////////////////////////////////
////                                                              ////
////  spi_top.v                                                   ////
////                                                              ////
////  This file is part of the SPI IP core project                ////
////  http://www.opencores.org/projects/spi/                      ////
////                                                              ////
////  Author(s):                                                  ////
////      - Simon Srot (simons@opencores.org)                     ////
////                                                              ////
////  All additional information is avaliable in the Readme.txt   ////
////  file.                                                       ////
////                                                              ////
//////////////////////////////////////////////////////////////////////
////                                                              ////
//// Copyright (C) 2002 Authors                                   ////
////                                                              ////
//// This source file may be used and distributed without         ////
//// restriction provided that this copyright statement is not    ////
//// removed from the file and that any derivative work contains  ////
//// the original copyright notice and the associated disclaimer. ////
////                                                              ////
//// This source file is free software; you can redistribute it   ////
//// and/or modify it under the terms of the GNU Lesser General   ////
//// Public License as published by the Free Software Foundation; ////
//// either version 2.1 of the License, or (at your option) any   ////
//// later version.                                               ////
////                                                              ////
//// This source is distributed in the hope that it will be       ////
//// useful, but WITHOUT ANY WARRANTY; without even the implied   ////
//// warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR      ////
//// PURPOSE.  See the GNU Lesser General Public License for more ////
//// details.                                                     ////
////                                                              ////
//// You should have received a copy of the GNU Lesser General    ////
//// Public License along with this source; if not, download it   ////
//// from http://www.opencores.org/lgpl.shtml                     ////
////                                                              ////
//////////////////////////////////////////////////////////////////////
```