Global Information Assurance Certification Paper

Information Assurance Ramifications of Using OpenSSL in the Department of Defense Computing Environment

By Joel I. Kirch

For SysAdmin, Audit, Network, Security (SANS) Global Information Assurance Certification (GIAC) GIAC Security Essentials Certification (GSEC) Certification Version 1.4b, Option 1

October 15, 2003

Table of Contents

Abstract

Open-source software now has the same standing in the Department of Defense as any other Commercial Off The Shelf (COTS) software. OpenSSL is a commercial-grade cryptographic library that is used by software developers and applications for many different types of encryption, not just SSL. Hewlett-Packard and the Open Source Software Institute are sponsoring the OpenSSL cryptographic library going to the DOMUS Information Technology Security Laboratory to be certified for FIPS 140-2. Because, the DCAS-1 security control from Department of Defense Instruction 8500.2 requires that all new Information Assurance acquisitions be certified, and FIPS 140-2 is one of the choices for certification, the OpenSSL cryptographic library makes a excellent choice.

This work will provide an overview of the new regulations that impact the use of an open-source cryptographic software library in the Department of Defense. This will be followed by a discussion of the OpenSSL cryptographic toolset functions as well as its licenses and the impact of what using such a cryptographic library could be for the Department of Defense.

Please note that some of the websites listed in this paper will require access from a .mil or .gov domain. In many cases, these same documents are available from other sources, but for the purpose of giving accurate source information, the original sources are listed. However, the main documents discussed, Department of Defense Directive 8500.1 and Department of Defense Instruction 8500.2, can found at the following URL and can be accessed from any domain: http://niap.nist.gov/cc-scheme/.

Background

The Department of Defense (DoD) is one of the largest computer environments in the world. Keeping these systems secure is the responsibility of many hard working Information Assurance professionals, so any tool that makes their job easier and security better should be considered.

OpenSSL is that tool; it is an excellent idea for the Department of Defense for many reasons. OpenSSL is a cryptographic library that supports the Secure Sockets Layer (SSL version 2 and version 3) and Transport Layer Security (TLS version 1) protocols. The OpenSSL website can be found at the following URL: http://www.openssl.org/. First, OpenSSL provides increased security by providing a standard set of cryptographic tools for Software Developers to use. The source code for OpenSSL is "open-source", which means that anyone is free to modify the code, as long as they abide by the terms of the license. Also, the OpenSSL cryptographic toolset is available at absolutely no cost to the Government, the Department of Defense, or the U.S. Taxpayer.

Before details of OpenSSL can be discussed, a foundation needs to be provided to show the basics of the regulations that affect Information Assurance acquisitions in the Department of Defense. The next section of the paper will address how OpenSSL complies with the Department of Defense's Information Assurance regulations.

Introduction to DoD Directive 8500.1

On October 24, 2002, the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence promulgated the Department of Defense Directive 8500.1. This regulation replaced:

- Department of Defense Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1998;
- Department of Defense 5200.28-M, "ADP Security Manual," January 1973;
- Department of Defense 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985.

The documents listed above have been canceled. For the purpose of maintaining the scope of this document, this paper will not provide more detail about the various laws and regulations that Department of Defense Directive 8500.1 is derived from. However, the 31 specific sources are listed in Enclosure E1 of the directive.

Department of Defense Directive 8500.1 replaced some very old and trusted regulations, which many people who have been practicing Information Assurance for a while have become accustomed to. However, many of the concepts remain the same. One of the most fundamental things that changed is the terminology. If a document

refers to the “C2 Level” or “ISSM / ISSO”, then that documentation has not been updated to reflect the changes in this new directive.

Information System Security Manager (ISSM) and Information System Security Officer (ISSO) have been replaced with the terms “Information Assurance Manager” (IAM) and “Information Assurance Officer” (IAO) respectively. The “C2 Level” terminology has been replaced with “Mission Assurance Categories” (MAC) and “Levels of Confidentiality.”

There are three Mission Assurance Categories: MAC I, MAC II, and MAC III. These categories define the system requirements for integrity and availability, where MAC I would have the most stringent requirements and MAC III, would have the least stringent requirements. Each Mission Assurance Category has a complimentary Confidentiality Level. The levels are also divided into three categories: Public, Sensitive, and Classified. Therefore, there are a total of nine possibilities for an Automated Information System to have using Department of Defense Directive 8500.1.

For example, a web-based system that is vital to providing information to the general public may be subject to the Mission Assurance Category I controls, because the system must always be available and the public needs to be sure of the integrity of the data. In addition, its Confidentiality Level may be Public because of the nature of the information it is providing.

As another example, a system that maintains the mailing addresses for a medical email list. It may be subject to Mission Assurance Category III controls because the loss of this system would not cause a significant impact to the readiness or effectiveness of its users, but because it deals with patient health information, the Confidentiality Level of the system may need to be Sensitive.

Department of Defense Directive 8500.1 had a lot of new ideas, but it did not provide the reader any clear way to implement these changes. The directive was very high-level and defined who was responsible for what, but Information Assurance professionals needed more details.

Better implementation details with DoD Instruction 8500.2

On February 6, 2003 Department of Defense Instruction 8500.2 was promulgated by the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence to address the implementation details that were lacking in Department of Defense Directive 8500.1. Department of Defense Instruction 8500.2 references:

- DoD 8500.1, “Information Assurance,” October 24, 2002;
- DoD 5025.1-M “DoD Directives System Procedures,” current edition;

- National Security Telecommunications and Information Systems Security Glossary Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000;
- DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002.

Again, for the purpose of maintaining the scope of this document, this paper will not provide more detail about the various laws and regulations that Department of Defense Instruction 8500.2 is derived from. However, the 32 specific sources are listed in Enclosure E1 of the instruction.

This instruction provided the implementation detail that was lacking in Department of Defense Directive 8500.1. There are 157 specific Information Assurance controls that are divided into 8 Information Assurance Control Subject Areas:

- Security Design and Configuration
- Identification and Authentication
- Enclave and Computing Environment
- Enclave Boundary Defense
- Physical and Environmental
- Personnel
- Continuity
- Vulnerability and Incident Management

From all of those 157 Information Assurance Controls, there is only one that directly deals with the use of open-source software:

> **DCPD-1 Public Domain Software Controls**
>
> "Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alterative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government." [Quoted from Department of Defense Instruction 8500.2]

The term DAA from the above quote refers to the Designated Approving Authority, this is the person formally accepts the residual security risks of deploying the system. The authors of the instruction did not specifically mention the words "open-source," however they clearly define the importance of the Government having access to the original source code. The fact that open-source software is specifically addressed in this

instruction, demonstrates that the authors considered its use in Department of Defense computer systems.

As was discussed in the SANS GSEC course, it would be very easy for a Cracker to add malicious code to a shareware or freeware application. The term "Cracker" and "Hacker" are being used as defined in The Jargon Dictionary, a Cracker is "*One who breaks security on a system*" and a Hacker is "*a person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.*" Tools such as "EXE Binder" allow Crackers to add their malicious code to existing executable files, making this type of hacking technique particularly effective.

Due to the fact that OpenSSL deals with cryptography, the Department of Defense Instruction 8500.2 controls that deal with encryption are listed in the table below (see Table 1).

DCNR-1 Non-Repudiation	NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.
DCAS-1 Acquisition Standards	The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources - the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation (See also DCSR-1).
ECCR-1 Encryption for Confidentiality (Data at Rest)	If required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.
ECCT-1 Encryption for Confidentiality (Data in Transit)	Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2).
ECNK-1 Encryption for Need-To-Know	Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality).

Table 1 – Encryption Controls from DoD I 8500.2

Again, for the purposes of maintaining the scope of this paper, these controls are just listed for completeness, however there are two items that are common to these controls that need further discussion. The terms NIST and FIPS need to be defined. NIST is the acronym for National Institute of Standards and Technology. Their mission is to "*develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.*" FIPS stands for Federal Information Processing Standards and these standards are maintained by NIST.

The Computer Security Resource Center, which is a division of the Information Technology Laboratory, Computer Security Division – part of NIST, is responsible for Computer Security Standards and Guidance. For example, they are currently drafting NIST Special Publication 800-61, Computer Security Incident Handling Guide which can be found at the following URL: http://csrc.nist.gov/publications/drafts/draft_sp800-61.pdf.

FIPS 140-2 "Security requirements for Cryptographic Modules" replaces FIPS 140-1, which has the same name. FIPS 140-2 discusses the joint agreement between the governments of the United States of America and Canada, whereby either country will accept the other's validated products. The program that both countries use is called the Cryptographic Module Validation Program (CMVP). More information about the CMVP can be found at the following URL: http://csrc.nist.gov/cryptval/. FIPS 140-2 defines the process for getting a cryptographic module validated, but to simplify for the purposes of this paper, FIPS 140-2 makes sure the mathematical algorithms for a particular encryption scheme are implemented correctly in the software. NIST maintains FIPS for many computer standards including popular encryption schemes used today such as: Advanced Encryption Standard (AES), Data Encryption Standard (DES), and the Digital Signature Standard (DSS).

It is very important for Information Assurance Officers and Managers, as well as Project Managers, to ensure that if a vendor claims that they have a FIPS 140-2 certified product, that the vendor provide written proof. This can be done by asking for the certificate number and verify it at the following website: http://csrc.nist.gov/cryptval/. If the vendor states that the product is on the pre-validation list then use the following URL for verification: http://csrc.nist.gov/cryptval/preval.htm.

Once a product is on the pre-validation list, which means a contract has been signed with an approved laboratory for the product to undergo testing, it is generally acceptable to use. However, check with the appropriate decision-makers in your organization.

This entire process is extremely complex and there are still some things that need to be addressed. For example, in requirement "DCAS-1 Acquisition Standards," any new Information Assurance product may only be purchased if it is on a validated products list from the following website: http://niap.nist.gov/cc-scheme/ValidatedProducts.html. According to that policy, cancel all of your purchases for any Anti-Virus software other than "Trend Micro InterScan™ VirusWall 3.52 for NT."

Unfortunately, as with most new policies, some clarification was needed. Luckily with regard to the use of open-source software in the Department of Defense a memorandum was quickly issued.

Department of Defense Memorandum on Open-Source Software

In an effort to address some of the confusion regarding open-source software, a memorandum from John P. Stenbit, (Assistant Secretary of Defense for Command, Control, Communications and Intelligence) was released on 28 May 2003, to clarify the Department of Defense position on open-source software. Mr. Stenbit was also the signing official for Department of Defense Instruction 8500.2.

The memorandum restated the Department of Defense current policy and provided some additional guidance. It restated the definition of open-source software and mentioned that Linux is an example of open-source software that is used within the Department of Defense. Linux is licensed under the GNU (GNU's Not Unix) General Public License (GPL), for a detailed explanation of the recursive GNU acronym and what it stands for please visit the following website: http://www.gnu.org/. The memorandum went into more detail when it stated that open-source software has to comply with the same Department of Defense policies that Commercial Off The Shelf (COTS) and Government Off The Shelf (GOTS) software does. Thus, open-source software now shares the same standing as any other COTS or GOTS software.

The Open-Source Software memorandum made the following key points: the software must comply with the National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP 11); the software must be configured properly with Department of Defense guidelines that are maintained by either Defense Information Systems Agency (DISA) or the National Security Agency (NSA); and because legal issues regarding licenses can be complex, you are advised to consult your legal group.

Details about NSTISSP 11 can be found at the following location: http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf. NSTISSP 11 basically just restates the “DCAS-1 Acquisition Standards” control from Department of Defense Instruction 8500.2. However, the next two items can be more of a problem for the Information Assurance Officer and Manager.

DISA and the NSA have developed security guidelines for configuring popular systems and hardware such as, Microsoft Windows 2000 Guide or a Cisco Router Guide from the NSA. The DISA guides, which require a .mil or .gov domain, can be found at the following URL: http://iase.disa.mil/policy.html. The NSA guides can be found at the following URL: http://www.nsa.gov/snac/. While these guides are very good for locking down those systems, they do not always keep up with the newest technology. For example, the NSA lists “Secure Configuration of the Apache Web Server, Apache Server Version 1.3.3 on Red Hat Linux 5.1,” considering that Red Hat 9 is the current version, more current standards should be considered. Industry standards, such as the

SANS “Securing Linux” guide could be used when the NSA or DISA does not have an available guide or it is out of date. The SANS “Securing Linux” guide can be found at the following URL: https://store.sans.org/store_category.php?category=consguides.

The encouragement to consult your legal group is a smart move for any Information Assurance professional; however, it may prove difficult finding someone who can answer your questions. Some Information Assurance professionals have contacted their legal groups only to find they needed to give a quick lesson on the differences in open-source software licenses and the details of the Open-Source Software memorandum. However, there is a person listed on the memorandum, who may be able to help.

Until now this paper has primarily discussed issues of policy and policy-implementation, but the title of the paper is “Information Assurance Ramifications of Using OpenSSL in the Department of Defense Computing Environment.” So, now that the foundation has been provided, more details about OpenSSL can be discussed.

OpenSSL

OpenSSL is a portable cryptographic toolset that is used for encrypting data. It is open-source, which means that anyone may look at the source code or modify it as they see fit. The reference to portability means that it will compile under both Microsoft Windows and all flavors of Unix and Linux. An example of the functionality the toolset provides is listed in Table 2, this table was derived from the following URL: http://www.openssl.org/docs/crypto/crypto.html:

Symmetric Ciphers	blowfish
	cast
	des
	idea
	rc2
	rc4
	rc5
Public Key Cryptography and Key Agreement	dsa
	dh
	rsa
Certificates	x509
	x509v3
Authentication Codes, Hash Functions	hmac
	md2
	md4
	md5
	mdc2
	ripemd
	sha

Table 2 – Sample of OpenSSL cryptographic functions supported

This cryptographic library is very complete and has been used in commercial applications. What makes this a benefit to the security community is that they can focus on what they want the application to do, and leave the implementation of the particular cryptographic functions to the OpenSSL library. For example, the OpenSSL cryptographic library can be used in other cryptographic applications such as OpenSSH, which provides a set of network connectivity tools that encrypt network traffic and serve as a secure replacement for telnet, rlogin, and ftp. Secure Shell (SSH) is the way that was recommended in the SANS GSEC course to communicate over a network.

The OpenSSL toolset has dual licenses, the "OpenSSL License" and the "Original SSLeay License." Both licenses apply to the source code, however they are structured like a BSD-style license. The Berkeley Software Distribution (BSD) license is the most forgiving of all of the licenses, basically you can do whatever you want with the source as long as you include the original copyright notice, also the software is provided on an "as-is" basis. The OpenSSL license is pretty forgiving too; it just has a little more restriction on using the "OpenSSL," "OpenSSL Project," and "OpenSSL Toolkit" names. The full contents of the licenses can be found at the following URL: http://www.openssl.org/source/license.html.

So, many software developers and integrators want to use OpenSSL because it is secure, open-source, and free. Also, many lawyers will probably allow you to use the OpenSSL library because it is no more restrictive than the Microsoft End User License Agreement (EULA). The EULA for Microsoft OfficeXP can be found at the following URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/office/officexp/reskit/html/eula.asp.

For some interesting reading comparing and contrasting the GPL, which is a popular license for many open-source software applications, and the Microsoft EULA visit the following URL: http://www.cyber.com.au/cyber/about/comparing_the_gpl_to_eula.pdf.

Unfortunately, at that point in time, the OpenSSL library would not have been able to be used because it did not meet the Department of Defense Instruction 8500.2 "DCAS-1 Acquisition Standards." The software did not meet any of the following requirements: "*International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program.*"

Benefits of OpenSSL becoming FIPS 140-2 validated

There was terrific news for Information Assurance professionals that were interested in using the OpenSSL library. On the 28th of April 2003 the Open Source Software Institute made a press release stating that "*OpenSSL Enters Evaluation for FIPS 140-2 Certification.*" Hewlett-Packard and the Open Source Software Institute are sponsoring the OpenSSL cryptographic library going to the DOMUS Information Technology

Security Laboratory (a NIST approved lab) to be certified for FIPS 140-2. Information about the Open Source Software Institute can be found at the following URL: http://www.oss-institute.org/oss-institute.com/www.oss-institute.org/index-2.html.

The "OpenSSL FIPS Cryptographic Module" is listed as number 76 and the vendor listed as the Open Source Software Institute on NIST's Cryptographic Module Validation Program for FIPS 140-1 and FIPS 140-2 Pre-Validation List, which can be found at the following URL: http://csrc.nist.gov/cryptval/140PreVal.pdf. Information about the FIPS 140-1 and 140-2 Pre-validation program can be found at the following URL: http://csrc.nist.gov/cryptval/preval.htm.

This is a huge benefit to the Department of Defense as well as the United States Taxpayer, because this cryptographic library is available for free. The OpenSSL project will be making the source code available in their main distribution when it is validated in the lab. There will be an option to compile it for FIPS 140-2 compliance. Software developers and integrators as well as Information Assurance professionals will be one step closer to being able to comply with Department of Defense Instruction 8500.2 "DCAS-1 Acquisition Standards."

To fully understand how vast a cost-savings this could be, the previous methodologies need to be briefly described.

Instead of paying a licensing fee for something like the "Oracle Crypto Library for SSL, version 9.0.4" from the Oracle Corporation, the software developer could just use the "OpenSSL FIPS Cryptographic Module" to handle all of the complex mathematics of getting the encryption correct and just focus on the software application's functionality, and it costs them nothing to use the OpenSSL library.

By having an open-source solution, competition is increased. It costs in the six-figure range to have something like the OpenSSL library validated, so it allows smaller companies to compete, and by allowing smaller companies to compete with large companies like Microsoft and Oracle, the Government should get increased innovation.

It saves the Government money too; typically the Government would need to have a vendor turn some Commercial Off The Shelf product into something customized for the Government to meet some security requirement. This new product is then called Government Off The Shelf, but it may have to be evaluated again, costing even more money.

OpenSSH and SSH Tectia are a notable example to illustrate the immense potential of OpenSSL becoming FIPS 140-2 validated. The OpenSSH project can be found at the following URL: http://www.openssh.org/. Information about the SSH Tectia product can be found at the following URL: http://www.ssh.com/products/tectia/. SSH Tectia is a product from SSH Communications Security, and it is also on the FIPS 140-2 pre-validation list. However, the SSH Tectia product is available for download for $133 USD per client. Compare that with OpenSSH, a product that has the same functionality and is

available to download for free. For Microsoft Windows implementations, Information Assurance professionals may want to use Cygwin, which contains both the OpenSSL and OpenSSH software, for free. The Cygwin project can be found at the following URL: http://www.cygwin.com/.

Because the OpenSSL cryptographic library is becoming FIPS 140-2 validated, the acquisition of Information Assurance products that use the OpenSSL library should become easier. It should save both time and money for the organization that has to pay for the National Security Agency or International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, or the NIAP Evaluation and Validation Program, because if additional security testing or validation of the software is required, the cryptography has already been validated by FIPS 140-2.

Lastly, a validated OpenSSL library will create more options for the Information Assurance professional. In a time when budgets are shrinking, and Information Assurance professionals are being asked to provide more security, OpenSSL provides one more option for providing defense-in-depth. By giving the people that design and maintain security for the Department of Defense this capability, a more robust security environment can be fostered.

Conclusion

To conclude, the Department of Defense memorandum regarding the use of open-source software clarified the Government position on using open-source software for Information Assurance professionals. OpenSSL is a commercial-grade cryptographic library that is used by software developers and applications for many different types of encryption, not just SSL.

Hewlett-Packard and the Open Source Software Institute are sponsoring the OpenSSL cryptographic library going to the DOMUS Information Technology Security Laboratory (a NIST approved lab) to be certified for FIPS 140-2. Given that Department of Defense Instruction 8500.2 (DCAS-1) requires that all new Information Assurance acquisitions be certified, and FIPS 140-2 is one of the choices for certification, the OpenSSL cryptographic library makes an excellent choice.

In addition, the Department of Defense, and the United States Taxpayer will save money because the OpenSSL cryptographic toolset is free. Many products that are based on this library are also free. For example, the SSH Tectia product is available for download at $133 USD per client, compared to OpenSSH (that uses the OpenSSL cryptographic library) which is available to download for free.

Finally, Information Assurance professionals will have more options for supporting the "defense-in-depth" methodology that is needed for one of the largest computer environments in the world because they will be able to consider open-source solutions that use the OpenSSL cryptographic library in their systems.

References

“A Comparison of the GPL and the Microsoft EULA.” Version 1,9 May 5, 2003 URL: http://www.cyber.com.au/cyber/about/comparing_the_gpl_to_eula.pdf

“Computer Security Resource Center.” URL: http://csrc.nist.gov/index.html

“Cygwin.” URL: http://www.cygwin.com/

“FIPS 140-2.” URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

"GNU's Not Unix.” URL: http://www.gnu.org/

"Information Assurance (IA)." Department of Defense Directive 8500.1 October 24, 2002. URL: https://lad.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf (.mil or .gov required)*

"Information Assurance (IA) Implementation." Department of Defense Instruction 8500.2 February 6, 2003. URL: https://lad.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf (.mil or .gov required)*

“Information Assurance Support Environment – Policy and Guidance.” URL: http://iase.disa.mil/policy.html (.mil or .gov required)

“Microsoft End User License Agreement for Office XP.” URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/office/officexp/reskit/html/eula.asp

“National Information Assurance Partnership.” URL: http://niap.nist.gov/cc-scheme/
*Please note that you can find DoDD 8500.1 and DoDI 8500.2 at this URL without originating from a .mil or .gov domain.

“National Information Assurance Partnership – Common Criteria Evaluation and Validation Scheme, Validated Products List.” URL: http://niap.nist.gov/cc-scheme/ValidatedProducts.html

“National Institute of Standards and Technology.” URL: http://www.nist.gov/

“National Security Agency -- Security Recommendation Guides.” URL: http://www.nsa.gov/snac/

“National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11.” January 2000 URL: http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf

"NIST Special Publication 800-61, Computer Security Incident Handling Guide." URL: http://csrc.nist.gov/publications/drafts/draft_sp800-61.pdf

"NIST Cryptographic Module Validation Program." URL: http://csrc.nist.gov/cryptval/

"NIST Cryptographic Module Validation Program FIPS 140-1 and FIPS 140-2 Pre-validation List." URL: http://csrc.nist.gov/cryptval/preval.htm

"NIST Cryptographic Module Validation Program FIPS 140-1 and FIPS 140-2 Pre-validation List." October 3, 2003 URL: http://csrc.nist.gov/cryptval/140PreVal.pdf

"OpenSSH." URL: http://www.openssh.org/

"OpenSSL – Documents -- Crypto." URL: http://www.openssl.org/docs/crypto/crypto.html

"OpenSSL – Source -- License." URL: http://www.openssl.org/source/license.html

"Open Source Software (OSS) in the Department of Defense (DoD) Memorandum." May 28, 2003. URL: http://iase.disa.mil/oss-in-dodmemo.pdf

"Open-Source Software Institute." URL: http://www.oss-institute.org/oss-institute.com/www.oss-institute.org/index-2.html

"SSH Secure Communications." URL: http://www.ssh.com/products/tectia/

"SysAdmin, Audit, Network, Security (SANS)." URL: https://store.sans.org/store_category.php?category=consguides

"The Jargon Dictionary." The Jargon File, version 4.2.2 20 August 2000 URL: http://info.astrian.net/jargon/