Global Information Assurance Certification Paper

NSTISSP No.11: Then and Now

GSEC Practical Assignment

Version (1.4b) Option 1

Billy Baker

June 24, 2004

Table of Contents

1.0 Abstract

National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11[1] is a simply written and easily followed document, and is neither cumbersome nor boring. It gives a clear understanding of a Defense-in-Depth Strategy to secure our Information Technology (IT) infrastructures. The policy has been through several revisions with very little actual change to the core of the document.

2.0 Introduction

Information Assurance (IA) has been separated into three distinct categories: People, Technology and Operations.

This paper will discuss one area within each category. It is important for all IA professionals to be conversant with each of these categories even though they are only briefly discussed in this paper.

The first category deals with the physical (People) aspect. It encompasses awareness, physical security, personnel security, system security, and administration.

They are not referenced in the order I listed, but when you review the fact sheet you will touch upon each of these subjects. I will provide two brief examples from the People category.

a) System Administration – If a person procures only accredited hardware and software from the Validated Products list, the first layer of system security has been accomplished.

b) Awareness – It is vital to have knowledge of current laws and policies along with changes as they occur, and to ensure that all documentation reflects these changes (e.g., Computer Security Act of 1987, Common Criteria, and NSTISSP No. 11).

The second category deals with Technology, which comprises IT/IA acquisition, risk assessments, C&A and technology Defense in-Depth. Products should conform to the Common Criteria specifications, ensuring that IT infrastructure remains protected. Before advising a company to purchase a product, it is important to ensure that the product provides confidentially, integrity, and availability, and the product have the right Protection Profile (PP), Security Target (ST). and required Evaluated Assurance Level (EAL).

[1] NSTISSP No. 11

The third category is Operations. This includes monitoring, intrusion detection, response and reconstitution. Whether the product purchased is hardware, software, or firmware, it has to be integrated into the current IT infrastructure. NSTISSP No. 11 provides the necessary guidance to accomplish this integration.

NSTISSP No. 11 is an often over looked document. I personally didn't know of its existence until a year ago, even though I have been in the IA field for a majority of my time in the military. I did not know of the NSTISSP No. 11 because everything in the military is filtered, or a "status quo" mindset is in place. When personnel report to a command, the infrastructure is already in place. All updates come from a single point that is trusted, so no one ever questions if the upgrades are accredited or approved by an outside entity such as Common Criteria or NIAP.

My interest in NSTISSP No. 11 has grown in recent months. I wanted to know all I could know about this document and its predecessors. I started with the 2000 version and compared it to the 2003 version. At first glance, it seems to be the same document, except the 2003 version adds couple of pages. After further review, I noticed some changes in the wording within the first three pages. The logical conclusion is that the older version should be discarded since it has obviously been superseded by the newer version. However, I was hesitant to do this since all the documents I dealt with in the military clearly stated when one document superseded another. NSTISSP No. 11 does not address this. Common sense would say the new version automatically supersedes the old version but common sense does not always prevail. People at my current job have both versions, causing much confusion within the organization. This paper will address some of the misconceptions about the two fact sheets of the two versions and the controversy that comes out of both.

The 2003 version contains only six pages but leads to much debate, interpretation, and controversy within the Information Assurance and Information Technology communities. In the project where I work, it has been the topic of some rather lively conversations. Prior to my arrival several months ago, my fellow IA professionals had no idea of the requirements or even the existence of this federal mandate, much less the magnitude of its ramifications on our current system and future expansion of our IT infrastructure.

NSTISSP No. 11 has caused several chokepoints within my section because of the mandate specifying that we can only select IA-enabled IT hardware and software products from a very short list provided by the federal government. Several of the most relevant passages are pulled from the NSTISSP No. 11 below:

> "(6) … IA and IA-enabled IT products to be used … on systems entering, processing, storing, displaying, or transmitting national security information. ….

(7) [T]he acquisition of all Commercial Off-the-Shelf (COTS) IA and IA-enabled IT products to be used on the systems specificed in paragraph (6), shall be limited only to those which has been evaluated and validated in accordance with [several international and national programs and agencies].

(11) Subject to policy and guidance for non-national security systems, departments and agencies may wish to consider the acquisition and appropriate implementation of evaluated and validated COTS IA and IA-enabled IT products.

(12) Heads of U.S. Departments and Agencies are responsible for ensuring compliance with the requirements of this policy." [1]

Even though the policy is spelled out very clearly in this federal mandate as well as Department of Defense Information Assurance Directive 8500.1, Section 4, subsection 4.17[2], we continue to debate the meaning of key words like "Agency", "National Security System" and "IA-enabled IT products." A broader interpretation would maximize our ability to select products from the Common Criteria Validated Products List (PPL)[3].

The questions that arise most often are, "Does it really affect us as a federal government/DOD project?" and, "Are we considered a National or non-National system?"

These are critical questions. If a network is defined as National, then NSTISSP No. 11 applies. If a network system is classified as a Non-National system, then NSTISSP No. 11 does not apply, but should be utilized under the "Best Practices" methodology.

Federal government 8500.1 directive has answered the question about the role and utilization of the NSTISSP No. 11. All organizations within the federal government must adhere to the accreditation process by verifying that the IT infrastructure only uses approved Commercial Off the Shelf (COTS) or Government Off the Shelf (GOTS) products after July 2002.

3.0 The Term "Agency"

Are the Departments of the Navy (and Marine Corps), Army, and Air Force considered federal agencies? This question is frequently debated where I work. To quote one of my senior managers about NSTISSP No. 11, "It doesn't apply to us because we are not a federal agency. We are part of the Department of the Navy." NSTISSP No. 11 does

[2] DOD 8500.1, Section 4, subsection 4.17
[3] Common Criteria

not specifically mention federal departments, and senior managers felt it therefore was not applicable.

However, the answer is that the military departments are part of the Department of Defense, which is one piece of the executive branch. They are, indeed, federal agencies.[4]

4.0 Definition of a National Security System

"A National Security System is any telecommunications or Automation Information System (AIS) operated by the United States government in which one of the following kinds of data is processed:

a) Military plans, weapons systems, or operations.

b) Foreign government information.

c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

d) Foreign relations or foreign activities of the United States, including confidential sources.

e) Scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism.

f) United States government programs for safeguarding nuclear materials or facilities.

g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism.

h) Weapons of mass destruction. " [5]

Networks that process one of these types of data must adhere to all federal mandates for network protection.

5.0 IA Products and IA-Enabled Products

It's not easy to discern the difference between IA-enabled products and IA products, and this difficulty frequently leads to confusion between them.

[4] Federal Executive Branch
[5] US Code, Title 40

"An IA product is an IT product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control and non-repudiation of data).

IA products include:

- Data Encryption
- Network Encryption
- Firewalls
- Intrusion Detection Devices

An IA -enabled product is a product or technology that provides security services, not as its primary role, but as an associated feature of its intended operating capabilities.

IA-enabled products include:

- Web browsers
- Screen routers
- Operating Systems (only use trusted systems)
- Secure Messaging System"[6]

6.0 Other Definitions

A National System is defined as a system by which administrative data is sent and received. Payroll, finance, logistics, and personnel management applications have their own laws and rules. The most pertinent law in this set concerns safeguarding private data, which is covered under the Privacy Act of 1974. Networks that process and store personal information should, per Para 11 of NSTISSP No. 11, still try to follow its guidelines as much as possible.

If your primary infrastructure is focused on the following definitions, then your system can be classified as a National System.

"Individual - a citizen of the United States or an alien lawfully admitted for permanent residence.

Maintain - includes maintaining, collecting, using, or disseminating.

Record - any item, collection, or grouping of information about an individual that is maintained, including, but not limited to, his/her education, financial transactions,

[6] NSTISSP #11 FAQs

medical history, and criminal or employment history, and that contains personal identification such as a name, identifying number or symbol, finger or voice print, or a photograph.

System of records - a group of any records under the control of any network from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[7]

7.0 Vendor and Manufacturer Responsibilities

Vendors and manufacturers of IT/IA products have different responsibilities today than a decade ago. Today's environment requires vendors to submit new operating system or network hardware products through a tough security process that has more stipulations than it did a decade ago.

Vendors deal with two distinct communities: the government, which has traditionally been more concerned with security (confidentiality), and the civilian sector, which has traditionally focused on data integrity. Today, both communities are starting to merge security philosophies. Both the civilian and government sectors want a product that can provide confidentially, integrity and availability.

Vendors and manufacturers are responsible for knowing the requirements and ensuring their products can pass the national and international standards.

Within the United States, all products must be accredited and certified by NIAP/Common Criteria and CMVP. This is mandatory for all vendors and product manufacturers wishing to do business with the government (all branches), not just the Department of Defense[8], and it is highly recommended that the civilian sector adopt the same Best Practice principles.

Vendors and manufacturers that market their IT solutions to the government must include the following critical items about their product:

- "Protection Profile (PP)

  A PP is a complete combination of security objectives, security-related functional requirements, information assurance requirements, assumptions, and rationale."[9]

[7] USDOJ Definitions
[8] DOD 8500.1, Section 4, subsection 4.17
[9] Protection Profile

- "Evaluated Assurance Levels (EAL)

  An EAL is a numerical designation of the confidence level in the security of the IT products and systems. There are currently seven levels that can be assigned to a vendor's product:

  EAL 1 (Functionally Tested)
  EAL 2 (Structurally Tested)
  EAL 3 (Methodically Tested and Checked)
  EAL 4 (Methodically designed, tested and reviewed)
  EAL 5 (Semi-formally designed & Tested)
  EAL 6 (Semi-formally verified designed and tested)
  EAL 7 (Formally verified designed and Tested). " [10]

  Note: EAL 4 is the minimum level that must be met by vendors' products if they wish to conduct any business with the United States government.

- "Security Targets (ST)

  STs are the vendor-provided documentation describing security aspects of the developed product."[11]

IA professionals who are assisting their company or command in purchasing products for either a new installation or infrastructure upgrade should be familiar with and understand the PP/EAL and ST functions.

A vendor must meet the following requirements prior to submitting a product for evaluation:

1. Develop and manufacture a product using the PP and EAL standards (assurance requirements).

2. Prepare an ST with PP standards (functional and assurance requirements).

Once the vendor believes the above requirements have been met, the product and documentation are submitted for evaluation to the NIAP/Common Criteria Board, which will then assign it to a certified testing lab for accreditation or certification.

This process could be costly and cumbersome, and it may take several months to get the final accreditation/certification. If you want to purchase this product, does this mean your organization cannot proceed forward? Not necessarily, because Para 13 of NSTISSP No. 11 allows some exceptions. I call it a grandfather clause but it's really not, although some within my organization have assumed it is. Para 13 has engendered a considerable amount of confusion.

[10] Evaluated Assurance Levels

For example, several months ago, our vendor provided us with an upgrade to our current operating system. After senior management agreed to go forward with the upgrade, they approached IA. Now, knowing NSTISSP No. 11 as I do, and constrained by both NSTISSP No. 11 and Department Of Defense Directive 8500.1, I asked the question, "Has the new upgrade been accredited via Common Criteria, or NIAP (FIPS 140) crypto-module?" I got looks of confusion and was asked to explain myself.

I informed senior management about both mandates, but weren't pleased with my explanation. One manager went online, pulled the 2000 version of NSTISSP No. 11 2000, read the whole three pages, and got stuck on Para 13, "IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirement of this policy." [12] He promptly reconvened the meeting and proceeded to tell us we don't fall under this regulation, that DOD 8500.1 doesn't apply because we are using the same vendor and same product. I again tried to explain that the follow-on sentence should be considered**: "**Information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions considered as replacement upgrades at the earliest opportunity."[13]

Most agreed to proceed with caution and to further investigate. However, we got hung up again, this time on Para 6, "Are we considered a National Security System?"

After all was said and done, the senior executive made the decision to have the vendor supply a "letter of integrity statement" in which the vendor indicated they would seek accreditation and certification for the operating system.

Two programs specifically listed in the SP 800-23[14] directive are key components used for testing commercial products. They are the National Information Assurance Program (NIAP)[15] Common Criteria Evaluation and Validation Program and NIST's Cryptographic Module Validation Program (CMVP)[16]. NIAP is the U.S. Common Criteria scheme, and CMVP is a program run jointly by NIST and the Canadian Security Establishment (CSE) for evaluating products against the FIPS 140-2 standard. Corsec specializes in both of these validations and offers classes to explain the procedures for successfully completing the validations. These are robust standards for a vendor to achieve, depending on the use of the product and the network transmitting and receiving the data.

---

[11] Security Target Development
[12] NSTISSP No. 11, Section "Exemptions and Deferred Compliance", Subsection 13
[13] NSTISSP No. 11, Section "Exemptions and Deferred Compliance", Subsection 13
[14] Roback, NIST Special Publication 800-23
[15] NIAP
[16] Cryptographic Module Validation Program

8.0 New Acquisitions

Products that have been through the Common Criteria/NIAP certification and validation process should be considered logical choices for products to be installed into a network. From a security and policy point of view, these are the ones I would recommend for procurement and to senior management. Within the federal government, all new acquisitions must have a PP. If the product does not yet have a validation certification, the vendor must supply documentation stating they will apply for validation via the Common Criteria.

If no PP exists for the selected product, it should not be considered, unless there is no other choice. In this case, the vendor will provide the following:

- An ST that describes the security features.
- A written statement that they will submit the product for validation to one of the accreditation agencies listed above.
- Proof that the product has obtained at least an EAL 2 status.

9.0 National Security Directive No. 42 (NSD-42)

> National Security Directive No. 42 entitled, "National Policy for the Security of National Security Telecommunications and Information Systems" (herein referred to as NSD-42), dated July 5, 1990, “establishes initial national objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding, from hostile exploitation, systems which process or communicate national security information; establishes a mechanism for policy development; and assigns responsibilities for implementation.” NSD-42 establishes an interagency group at the operating level, an executive agent, and a national manager to implement these objectives and policies. The National Security Telecommunications and Information Systems Security Committee (herein referred to as the NSTISSC or Committee) is established to consider technical matters and develop operating policies, guidelines, instructions, and directives, as necessary to implement the provisions of NSD-42. “[17]

The Committee on National Security Systems (CNSS) originated with NSD-42, which is responsible for the development of NSTISSP No. 11, along with the development and implementation of the following:

[17] NSD-42

- International Common Criteria for Information Security Technology, referred to as the Common Criteria within IA.
- National Security Agency (NSA)/National Information Assurance Partnership (NIAP).
- National Institute of Standards and Technology (NIST)
- Common Criteria Scheme

The Common Criteria Scheme is a concept that was originally designed and established as a interim agreement in 1997 between the United States of America, Canada, and Great Britian. Germany and France joined the Common Criteria a year later. Since 1998 several other countries have shown great interest in joining this organization to help institute national and international standards with one goal in mind: IT security.

Common Criteria is "intended to serve many communities of interest with very diverse roles and responsibilities. This community includes IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors, and accreditors (individuals deciding the fitness for operation of those products within their respective organizations). Close cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives"[18]

Common Criteria seeks to.

- Meet the security requirements of governments and commercial industry for cost-effective IT products that have been validated and certified.
- Develop secure testing programs.
- Ensure that all security evaluations of IA-enabled and IT products are performed to the same standards.
- Increase the availability of evaluated and certified IA-enabled and IT products.
- Eliminate duplicate IA-enabled and IT products in the market place.

Is Common Criteria good for the civilian sector? That has yet to be fully determined. Even though the private sector of the IT industry is starting to embrace the concept of Common Criteria, it still remains to be seen if full acceptance will ever happen. Cost and time to achieve a security certification via the Common Criteria is a major road

[18] Common Critieria

block, and unless it improves most of the civilian sector will not fully embrace Common Criteria.

The following is one of three sites that should be placed into the favorites list in every IA professional's browser:

NIAP Home | CCEVS Home | About Us | Contact Us | Help | Site Map | Jun 05, 2004

Available products to assist in making a more secure infrastructure.

- VPL (by Product Type)
- VPL (by Assurance Level)
- VPL (by Product Name)
- VPL (by Vendor)
- Archived Evaluated Products
- Products in Evaluation
- Validated Protection Profiles
- PPs in Development

Boosting consumer confindence through evaluation and testing of vendor products

- Getting a Product Evaluated
- Finding a CCTL
- Getting a CCTL Accredited

Policy that influences our adherence to the Common Criteria

- FEDERAL GOVERNMENT Directive #8500.1
- FEDERAL GOVERNMENT Instruction #8500.2
- NSTISSP No. 11, Revised Fact Sheet (July 2003)
- NSTISSP No. 11 Fact Sheet (Jan 2000)
- NIST Spec Pub 800-23
- NSD 42
- NSTISSAM Compusec/1-99
- USAF CIO Memorandum
- Pres. Decision Directive 63

For a comprehensive listing other pertinent IA-related docs, Click Here.

19

[19] Common Criteria

10.0 NIAP a Combination of NIST and NSA

NIAP originated from the combining of security experiences from the National Security Agency (NSA) and the National Institute of Standards and Technology. NIAP is a government sponsored program to oversee the security testing for both the buyers and vendors of IA-enabled IT products. NIAP is the best selection to oversee our IT infrastructures within the United States. The goals of NIAP are listed below.

NIAP seeks to:

- "Promote the development and use of evaluated IT products and systems.
- Development and use of national standards for IT security.
- Development in IT security requirements definition, test methods, tools, techniques, and assurance.
- Development and growth of a commercial security testing industry within the U.S.
- Oversee the certification of laboratories and testing of products under the Common Criteria evaluation and validation program."[20]

11.0 Computer Security Division of NIST

NIST has eight divisions, one of which is the Computer Security Division. It has several roles within the information system security arena. One of the key roles it has is with the crypto modules dealing with FIPS 140-1 and 2. The Computer Security Division also oversees the Cryptographic Module Validation Program (CMVP)[21], which validates cryptographic modules and algorithms. NIST and CMVP are the only references that an IA professional should use to see that vendors offering encryption services have acquired a validation certification for their products.

The FIPS 140-1 accreditation is being replaced by FIPS 140-2 accreditation. Products with FIPS-140-1 can still be used, but as crypto modules are upgraded, IA teams should start looking for FIPS 140-2 modules as replacements.

The following questions may come to mind as we reach this point. How much of a difference is there between the Common Criteria (CC) and NIST (CMVP) programs? Doesn't it seem to be redundant to have more than one organization doing validation? What happened to standardization, consistency and testing?

[20] National Information Assurance Partnership (NIAP)
[21] Cryptographic Module Validation Program

CMVP is the only organization that is allowed to test and certify crypto modules to ensure they are FIPS 140 complaint for use within a government run infrastructure. CMVP tests for conformance to four levels of security. FIPS 140 adopted a standard in 1994, and the four areas of testing were physical security, key management, roles and services, and self test. Common Criteria, as stated above, only tests for the PP and ST.

NIST (Computer Security Division) also brings the following to the IT security environment:

- Awareness of the ever-changing IT environment, so it can assist in identifying the latest IT risk, and vulnerabilities that we face in day to day operations.
- Security protection requirements, especially concerning new technologies.
- Assistance in development of standards, testing and design of metrics.
- Part of the overall scheme in the three organization accreditation process.
- Standards for all three branches of the Federal Systems

NIST CSD also provides an avenue for vendors seeking advice, technical guidance or assurance that the products they are producing meet security standards for all network environments, whether private or federal sector.

12.0 Summary

Throughout this paper, I have discussed different items within NSTISSP No. 11, from the federal mandate that requires us to use the process within No. 11 and adhere to its policy, to the roles of Common Criteria, NIAP, and NIST. Presidential and executive directives require the IA professionals and senior management of an organization to use the Common Criteria/NIAP or NIST for selection of network infrastructure, OS, and hardware. If a decision is made to ignore these mandates, then whoever made that decision should be considered a security risk to the organization and to the nation's Defense-In Depth strategy.

A lot has changed over the last decade, and IT security has come to the forefront, allowing no exception to the rules and no waivers to our security protocols. Our IT networks should be our first line of defense against threats from other nations and their wishes to do us harm. If we follow the simple rules instilled in NSTISSP No. 11 and only use the products that have been validated to provide that security, then we have accomplished the first layer in Defense In-Depth.

References

National Security Agency. "NSTISSP No. 11 - Fact Sheet for the National Assurance Information Acquisition Policy." Section "Exemptions and Deferred Compliance", Subsection 13. July 2003 URL:http://www.nstissc.gov/Assets/pdf/nstissp_11_fs.pdf

Department of Defense. "DIRECTIVE NUMBER 8500.1." Section 4, "Policy." Subsection 4.17. Page 7. 24 Oct 02. URL: http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf (21Nov 03)

National Institute of Standards and Technology. "The Common Criteria Evaluation and Validation Scheme." "Validated Products List (VPL)."URL: http://niap.nist.gov/cc-scheme/vpl/vpl_type.html (02 July 2004)

The U. S.Government's Official Web Portal. "Federal Executive Branch." Firstgov.gov. URL: http://www.firstgov.gov/Agencies/Federal/Executive.shtml (2004)

Legal Information Institute. "US Code, Title 40, Chapter 25, Section 1452." URL: http://www4.law.cornell.edu/uscode/40/1452.html (2004)

National Institute of Standards and Technology. "The Common Criteria Evaluation and Validation Scheme." "NSTISSP #11 Frequently Asked Questions." URL:http://niap.nist.gov/cc-scheme/nstissp-faqs.html#Q33 (02 July 2004)

U.S. Department of Justice. "Overview of the Privacy Act of 1974." "Definitions." URL:http://www.usdoj.gov/04foia/04_7_1.html (May 2004)

Department of Defense. "DIRECTIVE NUMBER 8500.1." Section 4, "Policy." Subsection 4.17. Page 7. 24 Oct 02. URL: http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf (21Nov 03)

The National Security Agency. "Protection Profiles." URL: http://niap.nist.gov/pp/index.html (16 June 2004)

Infosec Assurance and Certification Services. "Common Criteria Assurance Levels." URL: http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=13 (2003)

TNO ITSEF BV. "Security Requirement Definitions." "Security Target Development." URL: http://www.commoncriteria.nl/requirements.html (24 Jun 2004)

National Security Agency. "NSTISSP No. 11 - Fact Sheet for the National Assurance Information Acquisition Policy." Section "Exemptions and Deferred Compliance", Subsection 13. July 2003
URL:http://www.nstissc.gov/Assets/pdf/nstissp_11_fs.pdf

National Security Agency. "NSTISSP No. 11 - Fact Sheet for the National Assurance Information Acquisition Policy." Section "Exemptions and Deferred Compliance", Subsection 13. July 2003
URL:http://www.nstissc.gov/Assets/pdf/nstissp_11_fs.pdf

Roback, Edward. "NIST Special Publication 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products." U.S. Department of Commerce. URL:
http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf (Aug 2000)

The National Security Agency. "NIAP." URL: http://niap.nist.gov/ (16 June 2004)

Computer Security Division National Institute of Standards and Technology. "Cryptographic Module Validation Program." NIST. URL:
http://csrc.nist.gov/cryptval/ (08 Mar 2004)

"National Security Directive No. 42"
URL:http://www.fas.org/irp/offdocs/nsd/nsd_42.htm (01 Apr 1992)

National Institute of Standards and Technology. "The Common Criteria Evaluation and Validation Scheme." URL: http://niap.nist.gov/cc-scheme/policy/ccevs/scheme-pub-5.pdf

National Institute of Standards and Technology. "The Common Criteria Evaluation and Validation Scheme." URL:http://niap.nist.gov/cc-scheme/index.html (24 Jun 2004)

Computer Security Division National Institute of Standards and Technology. "Cryptographic Module Validation Program." NIST. URL:
http://csrc.nist.gov/cryptval/ (08 Mar 2004)