NIST Special Publication 800-23

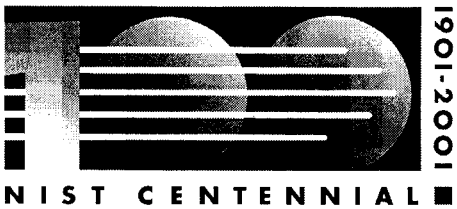
U.S. DEPARTMENT OF
COMMERCE
Technology Administration
National Institute of Standards
and Technology

Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Recommendations of the National Institute of Standards and Technology

Edward A. Roback

C O M P U T E R S E C U R I T Y



NIST National Institute of Standards and Technology • Technology Administration • U.S. Department of Commerce

NIST Special Publication 800-23

Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Recommendations of the National Institute of Standards and Technology

Edward A. Roback

C O M P U T E R S E C U R I T Y

Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2000

U.S. Department of Commerce
Norman Y. Mineta, Secretary

Technology Administration
Dr. Cheryl L. Shavers, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Raymond G. Kammer, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-23
Natl. Inst. Stand. Technol. Spec. Publ. 800-23, xx pages (Aug. 1999)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2000

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402-9325

Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Recommendations of the National Institute of Standards and Technology

Purpose

This document provides guidelines for Federal organizations' acquisition and use of security-related Information Technology (IT) products. NIST's advice is provided in the context of larger recommendations regarding security assurance.

Authority

This document has been developed by NIST in furtherance of its statutory responsibilities (under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996, specifically 15 U.S.C. 278 g-3(a)(5)). This is not a guideline within the meaning of (15 U.S.C. 278 g-3 (a)(3)).

These guidelines are for use by Federal organizations which process sensitive information.[1] They are consistent with the requirements of OMB Circular A-130, Appendix III.

The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon Federal agencies by the Secretary of Commerce under his statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other Federal official.

Background

These guidelines provide advice to agencies *for sensitive (i.e., non-national security) unclassified systems*. This advice regarding sensitive unclassified systems complements

[1] Many people think that sensitive information only requires protection from unauthorized disclosure. However, the Computer Security Act provides a much broader definition of the term "sensitive information:" *any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.*

the guidance recently issued for the *national security* community for the use and acquisition of "information assurance" products.

In January 2000, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) issued National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products." NSTISSP Number *11 applies to national security systems* as defined in National Security Directive 42. A summary of NSTISSP Number 11 appears in Appendix I for reference purposes. The complete document is available to Government organizations through the NSTSSC Secretariat (I42), National Security Agency, 9800 Savage Road, Ft. Meade, MD, 20755-6716.

Guidelines

1. **Federal departments and agencies should understand the concept of computer security assurance.**

Broadly speaking, computer security assurance provides a basis for one to have confidence that security measures, both technical and operational, work as intended. Varying degrees of assurance[2] are supported through methods such as conformance testing, security evaluation, and trusted development methodologies. Assurance is not, however, a guarantee that the measures work as intended; it is closely related to areas of reliability and quality.[3]

2. **Federal departments and agencies should be aware of how assurance in the acquired products supports security.**

In general, the higher the assurance, the greater the confidence a manager has that the IT products, systems, networks being used work as intended and are being sufficiently protected.[4] Assurance in individual product components contributes to overall system security assurance – but it neither provides a guarantee of system assurance nor, in and of itself, secures a system. Use of products with an appropriate degree of assurance contributes to security and assurance of the system as a whole and thus should be an important factor in IT procurement decisions. For a security product, system or software a combination of measures for such areas as security functionality, sound development and operational practices, and periodic inspection and review, needs to be addressed as well. In other words, complementary and interdependent controls are needed, such as sound operating procedures, adequate training, comprehensive policies, sound security architectures, and a comprehensive risk management program.

---

[2] The term "assurance" is used throughout as shorthand for "security assurance."

[3] Details regarding the definition of assurance and examples of how it can be obtained can be found in NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook" available at http://csrc.nist.gov/nistpubs/.

[4] Sufficient protection refers to the level of security deemed so by the management official who authorizes a system to process information, (some agencies refer to this authorization as accreditation). See Appendix III to OMB Circular A-130.

3. **Federal departments and agencies should be knowledgeable of the many approaches to obtaining security assurance in the products they procure.**

There are a number of ways that security assurance in products and systems is achieved/determined, such as:

NIST, NSA or other Conformance Testing and Validation Suites
Testing and Certification
Evaluation and Validation
Advanced or Trusted Development Techniques
Performance Track Record/Users' Experiences
Warranties, Integrity Statements, and Liabilities
Secure Distribution

Note that the reliability of these methods can vary considerably. See Chapter 9 entitled "Assurance" in *An Introduction to Computer Security: The NIST Handbook NIST Computer Security Handbook* and the Common Criteria general information web page at *http://csrc.nist.gov/nistpubs/ and http://niap.nist.gov/cc-scheme* for a more in-depth discussion.

4. **Federal agencies should specifically be aware of the benefits that can be obtained through testing of commercial products against customer, government, or vendor-developed specifications.**

Two Government programs are of particular interest here – the National Information Assurance Partnership (NIAP)'s Common Criteria Evaluation and Validation Program and NIST's Cryptographic Module Validation Program (CMVP). The NIAP program focuses on *evaluations* of products (e.g., a firewall or operating system) against a set of security specifications. The CMVP program focuses on security *conformance testing* of a cryptographic module against Federal Information Processing Standard 140-1, *Security Requirements for Cryptographic Modules* and related Federal cryptographic algorithm standards.

The **NIST / NSA – sponsored NIAP** is a U.S. Government initiative designed to meet the security evaluation needs of both IT producers and consumers. The NIAP program is intended to foster the availability of objective methods for evaluating the security of IT products. In addition, NIAP is designed to foster the development of commercial testing laboratories that can provide the types of testing and evaluation services which will meet the demands of both producers and consumers. The NIAP focuses on evaluations conducted in accordance with the "Common Criteria" (ISO/IEC 15408) evaluation approach. In addition to containing a taxonomy of security functional requirements, the "Common Criteria" specifies seven predefined assurance packages, known as Evaluation Assurance Levels (EALs). While these may be more generally well-known, the Common Criteria provides the flexibility to allow producers and consumers to define their unique assurance requirements (i.e., use of one of the predefined EALs is not mandatory.)

Agencies may use the laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform evaluations of products against security requirements expressed using the "Common Criteria." As the NIAP progresses, such security requirements, known as "protection profiles" will be developed by industry and government consumers. For those security requirements which may be appropriate to a broad segment of its Federal community, NIST intends to generally promulgate protection profiles as technical guidelines to the Federal community following an informal agency review and comment process. Testing can also be accomplished against vendor-developed security requirements associated with a vendor's specific product or system, known as a "security target." This testing can support vendor security claims. The evaluation conducted by accredited private sector laboratories under the auspices of NIAP provides for varying levels of assurance, to meet customer requirements. (See http://niap.nist.gov.)

The **Cryptographic Module Validation Program** (CMVP), which is jointly run with the Government of Canada's Communications Security Establishment, provides customers with assurance, through functional testing, that:

1) a cryptographic module meets one of the four security specification levels of Federal Information Processing Standard 140-1, *Security Requirements for Cryptographic Modules* (a mandatory Federal Information Processing Standard for sensitive (unclassified) applications and

2) that the FIPS-approved algorithms (e.g., Triple DES) are correctly implemented.

Assurance of the proper functioning of cryptographic modules and algorithms is considered critical because encryption techniques are used to protect sensitive data that is transmitted over untrusted paths (e.g., over the Internet). Additionally, the knowledge of and consequences resulting from unauthorized disclosure of information may not be apparent for some time (as compared, say, to the immediate awareness that a homepage has been defaced). The specifications for FIPS 140-1 and a current list of validated modules can be found at http://csrc.nist.gov/cryptval/

CMVP tested modules are often integrated into commercial products with additional (i.e., non-cryptographic) functionality. The assurance provided by CMVP concerning cryptographic modules does not imply assurance with regard to other aspects of the product into which the module is incorporated. The CC-NIAP evaluation approach described can be used to complement the CMVP (i.e., to evaluate other security requirements of the product), thereby addressing assurance of the overall product.

5. **Federal departments and agencies should acquire and use products appropriate to their risk environment and the cost-effective selection of security measures. Agencies should develop policies for the procurement and use of evaluated products as appropriate. When selecting products, agencies need to consider the**

threat/risk environment, cost-effectiveness, assurance level, and security functional specifications, as appropriate.

A listing of products which have been validated under the NIAP's Common Criteria Evaluation and Validation Program can be found via http://niap.nist.gov. At the time of this writing, no Common Criteria protection profiles have been designated as mandatory and binding by the Secretary of Commerce. It is NIST's intent to issue protection profiles (when appropriate) as technical security guidelines to the Federal community.

With specific regard to ***cryptographic modules and FIPS-approved cryptographic algorithms***, agencies are reminded that the use of modules tested as conformant to *Security Requirements for Cryptographic Modules* (Federal Information Processing Standard 140-1) has been made mandatory and binding by the Secretary of Commerce. NIST maintains a publicly available list of modules, which have been so validated, at http://csrc.nist.gov/cryptval/ .

6. **Federal Agencies should give substantial consideration in IT procurement and deployment for IT products that have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements. Examples of these specifications will include NIST recommended protection profiles based on ISO/IEC 15408, the Common Criteria.**

The ultimate goal in purchasing a system is to obtain the necessary functionality and performance within cost and time constraints. Moreover, performance includes dependability and reliability and hence is directly impacted by security considerations. In general, third party testing and evaluation provides a significantly greater basis for customer confidence than many other assurance techniques. Yet, it is important to note that purchasing an evaluated product simply because it is evaluated and without due consideration of applicable functional and assurance requirements, may be neither useful nor cost effective. IT users need to consider their overall requirements and select the best products accordingly.

7. **Federal departments and agencies need to address how products (with appropriate assurance) are configured and integrated properly, securely and subject to the managerial operational approval process[5] so as to help ensure security is appropriately addressed on a system-wide basis.**

The overall assurance level of a system as a whole may be different (usually lower) than the assurance level of individual components. While product assurance is a crucial and necessary input into the system security process, all the usual policies, controls, and risk management processes must also be in place for a system to operate in a reasonably secure mode. There are typically specific configuration settings that must be employed for the product to operate in the secure manner desired. In addition, much attention must be paid to combining such products in order to provide an appropriate security solution

[5] This refers to the approval process discussed in Office of Management and Budget Circular A-130, Appendix III.

for a given risk and threat environment. Thus, in addition to employing products with appropriate security capabilities and assurance, review of the security of a system from a system-wide perspective supports the managerial operational approval process.

Agencies should also be aware of the interconnectivity and associated interdependence of organizations and that a risk accepted by one organization may inadvertently expose other organizations to the same risk.

Supplemental Information

Appendix I: *Fact Sheet -- National Security Telecommunications and Information Systems Security (NSTISSP) Number 11, National Information Assurance Acquisition Policy.* (NSTISSP Number 11 itself is "For Official Use Only" and therefore not included in this document.)

Appendix II: *National Security Telecommunications and Information Systems Security Committee Advisory Memorandum for the Strategy for Using the National Information Assurance Partnership (NIAP) for the Evaluation of Commercial Off-the-Shelf (COTS) Security Enabled Information Technology Products.* (NSTISSAM INFOSEC/2-00)

FACT SHEET

NSTISSP No. 11

National Information Assurance Acquisition Policy

January 2000

Background

(1) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products is issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

(2) The NSTISSC was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems.

Introduction

(1) The technological advances and threats of the past decade have drastically changed the ways we think about protecting our communications and communications systems. Three factors are of particular significance:

- The need for protection encompasses more than just confidentiality;
- Commercial off-the-shelf (COTS) security and security-enabled information assurance (IA) products are readily available as alternatives to traditional NSA-developed and produced communications security equipment (i.e., government-off-the shelf (GOTS) products); and
- An increased and continuing recognition that the need for IA transcends more than just the traditional national security applications of the past.

NSTISSC Secretariat (I42) • National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716
(410) 854-6805 OR Toll Free 1-888-NSTISSC• UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

(2) In the context of the second of the above factors, it is important that COTS products acquired by U.S. Government Departments and Agencies be subject to a standardized evaluation process which will provide some assurances that these products perform as advertised. Accordingly, the attached policy has been developed as a means of addressing this problem for those products acquired for national security applications. The policy also rightfully points out that protection of systems encompasses more than just acquiring the right product. Once acquired, these products must be integrated properly and subject to an accreditation process which will ensure total integrity of the information and systems to be protected.

Policy

(1) Information Assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated Government Off-the-Shelf (GOTS) or Commercial Off-the-Shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products should provide for the *availability* of the systems; ensure the *integrity* and *confidentiality* of information, and the *authentication* and *non-repudiation* of parties in electronic transactions.

(2) Effective 1 January 2001, preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which have been evaluated and validated, as appropriate, in accordance with:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;

- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or

- The NIST Federal Information Processing Standard (FIPS) validation program.

(3) The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

(4) By 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in paragraph (2), above, shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the three sub-bullets.

(5) The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information shall be limited to products which have been evaluated by the NSA, or in accordance with NSA-approved processes.

(6) Normally, a complementary combination of IA/IA-enabled products is needed to provide a complete security solution to a given environment. Thus, in addition to employing evaluated and validated IA/IA-enabled products, a solution security analysis should be conducted as part of the certification and accreditation process. In support of this, NSA shall provide guidance regarding the appropriate combinations and implementation of GOTS and COTS IA and IA-enabled products.

(7) 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. The use of these products may be appropriate for systems which process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation and/or maintenance of critical infrastructures as defined in Presidential Decision Directive No. 63 (PDD-63), Critical Infrastructure Protection.

Responsibilities

(8) Heads of U.S. Departments and Agencies are responsible for ensuring compliance with the requirements of this policy.

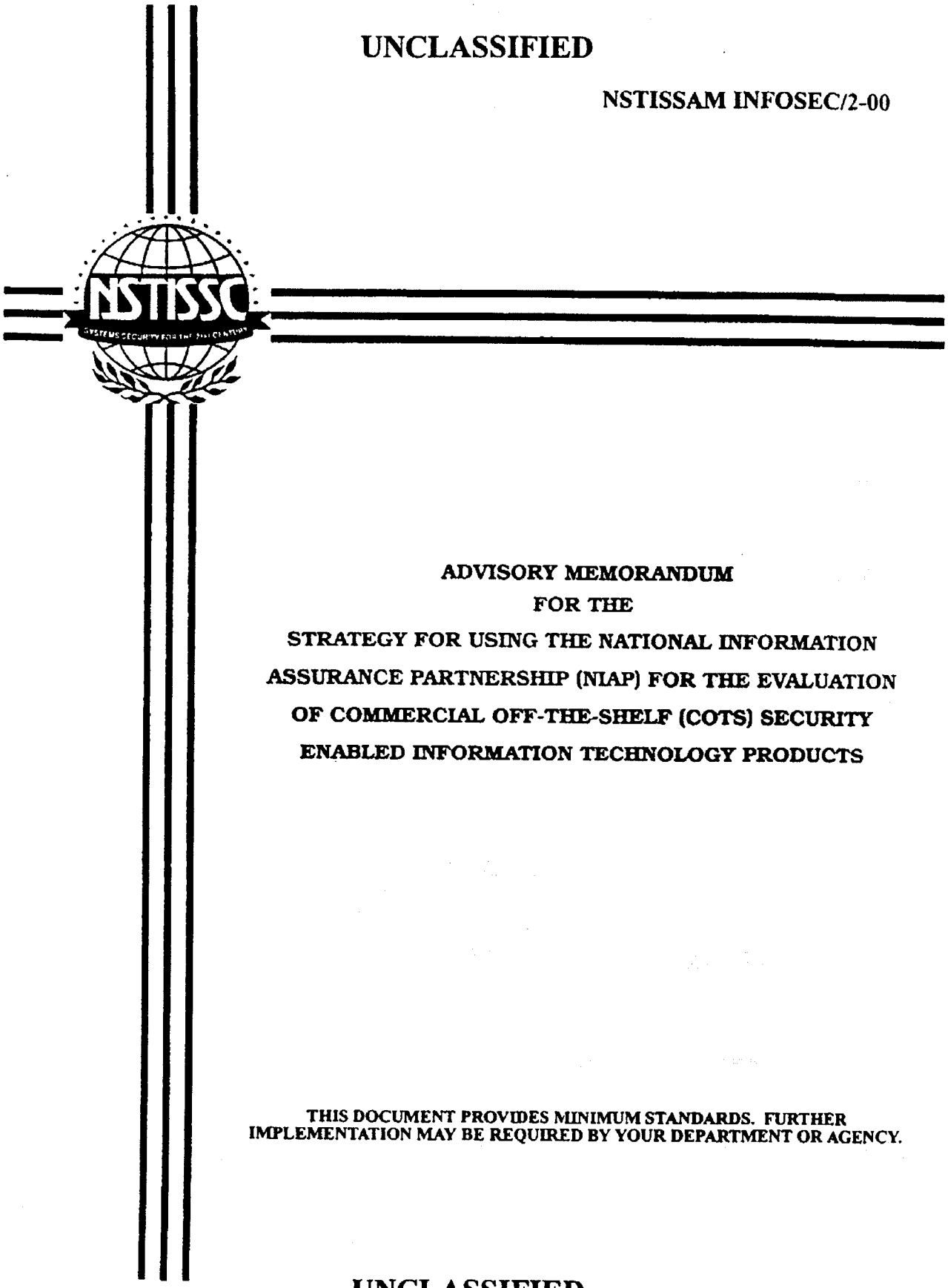
Exemptions and Waivers

(9) COTS or GOTS IA and IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirements of this policy. 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.

(10) Waivers to this policy may be granted by the NSTISSC on a case-by-case basis. Requests for waivers, including a justification and explanatory details, shall be forwarded through the Director, National Security Agency (DIRNSA), ATTN: V1, who shall provide appropriate recommendations for NSTISSC consideration. Where time and circumstances may not allow for the full review and approval of the NSTISSC membership, the Chairman of the NSTISSC is authorized to approve waivers to this policy which may be necessary to support U.S. Government operations which are time-sensitive, or where U.S. lives may be at risk.

UNCLASSIFIED

NSTISSAM INFOSEC/2-00



ADVISORY MEMORANDUM FOR THE STRATEGY FOR USING THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP) FOR THE EVALUATION OF COMMERCIAL OFF-THE-SHELF (COTS) SECURITY ENABLED INFORMATION TECHNOLOGY PRODUCTS

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

UNCLASSIFIED

National Security Telecommunications and Information Systems Security Committee

NATIONAL MANAGER

FOREWORD

1. This Advisory Memorandum provides guidance to U.S. Government departments and agencies regarding the strategy behind the National Information Assurance Partnership (NIAP) for the evaluation of commercial off-the-shelf (COTS) security enabled information technology products and, from a practical standpoint, details its implementation. It also serves to document the respective roles of the National Security Agency (NSA), the National Institute of Standards and Technology (NIST) and the accredited laboratories in the overall COTS evaluation and validation process.

2. Issuance of the document represents another step in a continuing effort to keep departments and agencies apprised of significant information systems security or information assurance developments which may impact on the operations and activities of their respective organizations. This advisory supplements information previously published on the evaluation of COTS products which was published in NSTISSAM COMPUSEC/1-99, Subject: Advisory Memorandum on the Transition From the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation, dated 11 March 1999.

Michael V. Hayden

MICHAEL V. HAYDEN
Lieutenant General, USAF

NSTISSC Secretariat (I42) • National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716
(410) 854-6805 • UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

ADVISORY MEMORANDUM
ON THE
STRATEGY FOR USING
THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP)
FOR THE EVALUATION OF COMMERCIAL OFF-THE-SHELF (COTS)
SECURITY ENABLED INFORMATION TECHNOLOGY PRODUCTS

SECTION I - REFERENCES

a. NSTISSAM COMPUSEC/1-99, Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria (TCSEC) to the International Common Criteria for Information Technology Security Evaluation, dated 11 March 1999

b. NSTISSAM COMPUSEC/1-98, The Role of Firewalls and Guards in Enclave Boundary Protection, dated December 1998

SECTION II - GENERAL BACKGROUND

1. Reference a. provided guidance to U.S. Government departments and agencies on the transition from the Trusted Computer System Evaluation Criteria (better known as the Orange Book) to the International Common Criteria as the basis for evaluation of commercial off-the-shelf (COTS) security and security-enabled information technology (IT) products. It further advised that the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) had established the National Information Assurance Partnership (NIAP) to accredit private sector laboratories to evaluate products and systems in accordance with the Common Criteria.

2. This advisory provides additional information on the NIAP process for evaluating COTS security and security-enabled IT products, the NIAP product certificate, and the NIAP Validated Products List (VPL). Additionally, this advisory provides guidance on the NSA strategy to use the Common Criteria and the NIAP to certify security and security-enabled IT products for the national security community.

SECTION III - THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP

3. The NIAP is a collaborative effort between NIST and NSA designed to meet the security evaluation needs of both IT producers and users. The program fosters the availability of standardized specifications and test methods for evaluating the security robustness of COTS security and security-enabled IT products. In addition, it is designed to foster the development of commercial testing laboratories to provide security evaluation services which will meet the demands of both producers and users. NIAP testing will replace the COTS IT product evaluations previously performed by NSA under the Trusted Product Evaluation Program (TPEP) and other programs.

4. The NIAP program requires an extensive accreditation process for all commercial laboratories. This process, performed by the National Voluntary Laboratory Accreditation Program (NVLAP), an internationally recognized accreditation body, analyzes the laboratory quality processes against the International Standards Organization (ISO) Guide 25 and ISO

9000 quality principles. Additionally, the laboratories are analyzed and tested on their ability to interpret and apply the Common Criteria (CC) and its associated Common Evaluation Methodology. Once accredited by NVLAP and accepted by NIAP into the program, a laboratory will contract directly with a sponsor (usually a product manufacturer) to have a security or security-enabled IT product evaluated. NIAP assigns a government validator to each product evaluation to monitor the laboratory compliance with the CC as well as the quality and consistency of work being performed.

5. The laboratory will evaluate the product against a Security Target (ST) provided by the vendor. The ST is a CC-based document which describes the product's security functionality claims, as well as the desired level of evaluation (specified as an Evaluated Assurance Level (EAL)) that the laboratory performs to verify whether the product meets its security claims. If the product meets the ST criteria, the laboratory issues a report to NIAP documenting the results of the analysis performed by the laboratory. NIAP reviews the laboratory report to determine if the analysis was consistent with CC requirements. If consistent, NIAP will issue a certificate to the sponsor of the evaluation validating that the product is consistent with the claims in the ST. This certificate is signed by the NIST and NSA senior level executives responsible for the NIAP program and the product is listed on the NIAP VPL which can be found at:

http://niap.nist.gov/cc-scheme/ValidatedProducts.html

6. **Important:** Products listed on the NIAP VPL should not be interpreted as an NSA or a NIST endorsement or certification of the product for government use. It is only a validation that the product met its security claims consistent with the level of analysis performed by the laboratory and that the laboratory analysis performed was consistent with CC and Common Evaluation Methodology requirements. For example, a product may claim that it performs access control using a password entry system with a two character password. If the laboratory finds that indeed the product provides access control using a two character password, the product has successfully met its claim and would be awarded a certificate signed by NIST and NSA. However, this does not mean that either NIST or NSA endorse a product employing a two character password as appropriate for government access control requirements.

7. **Important:** Security vulnerabilities may exist in a product for which a validation certificate was issued by NIAP if such vulnerabilities would have been only discovered as a result of a level of evaluation (i.e., EAL) higher than that specified in the security target. Government integrators are advised to carefully read the ST and NIAP validation report to determine if the product security functionality and evaluation level performed is appropriate for a specific application.

SECTION IV - USE OF NIAP FOR THE EVALUATION OF COTS SECURITY AND SECURITY-ENABLED IT PRODUCTS

8. The migration from NSA evaluation of COTS products to the NIAP evaluation program is based upon several factors. Over the past decade, there has been a tremendous growth in the availability of COTS security and security-enabled IT products, and a corresponding increasing demand for these products to be evaluated. This increased availability of products, coupled with rapid product updates and new releases, has led to a dramatic increase in the time required to service evaluation requests. When completed, the evaluation was often outdated as the evaluated version of the product was no longer supported by the manufacturer. A move to commercial evaluation facilities will allow evaluations to be

performed at a faster rate than previous NSA evaluations as commercial laboratories are able to react more quickly to market demands.

9. In order to achieve fairness in the market place and to avoid government competition with the NIAP commercial laboratory evaluation program, NSA will no longer service customer requests for the evaluation of COTS security or security-enabled IT products. Government customers should look to the NIAP program for their security and security-enabled COTS IT product evaluation requirements. NSA will continue to evaluate U.S. Government-developed security products, as well as augment COTS evaluations higher than EAL4 provided they have first undergone a preliminary NIAP evaluation.

SECTION V - GUIDANCE REGARDING THE USE OF SECURITY AND SECURITY-ENABLED COTS IT PRODUCTS

10. To provide customer guidance on recommended minimum essential security robustness requirements for security and security-enabled COTS IT products, NSA will issue a series of technology-based Common Criteria (CC) Protection Profiles. These Protection Profiles are being developed under the auspices of the Information Assurance Technology Framework (IATF) in cooperation with the user community and security vendors. More detailed information on the IATF is available at:

http://www.iatf.net

Recommended protection profiles for firewalls were previously addressed in reference b., and are available at:

http://www.radium.ncsc.mil/tpep/

Protection Profiles are also being developed for levels of robustness designated as:

a. Basic
b. Medium
c. High

11. Protection profiles will take into account the sensitivity of the data, the level of threat, the state of the art of COTS security products, and the cost and time for an evaluation to be completed.

Important: It must be emphasized that security products which meet these profiles may still contain vulnerabilities. Nevertheless, the profiles will be the best that can be accomplished at the present time based upon the rate of change and the maturity of COTS security product development processes. In designing Protection Profiles for differing levels of robustness, the threat to the information is addressed based upon the value of the information as well as the environment in which the product will be placed. For example, the level of value of classified information is defined to be higher than that for unclassified data. Similarly, the scope of evaluation specified in the protection profiles is based upon the threat perceived to the data in that environment. Additionally, the scope of evaluation must also take into account the economic costs in performing that evaluation in terms of dollars and time and the existing state of the art of COTS security and security enabled technology. For example, while it may be desirable to perform a full source code analysis on all firewalls destined for an unclassified but sensitive-mission support data environment, the economic costs of such an analysis when weighed against the value of this information makes this approach untenable. Firewall vendors

are not willing to pay the attendant costs for this type of evaluation, and it is unlikely that any such evaluation could be accomplished before a new version of the firewall would be released.

SECTION VI - NSA CERTIFICATIONS

12. NSA will certify Protection Profiles determined to be compliant with the IATF. Protection Profiles so certified will be identified on the NSA home page at:

http://www.radium.ncsc.mil/tpep

Additionally, where a protection profile does not exist, government customers may request NSA to review and certify vendor security targets (STs) to determine if the product's proposed security functionality and level of evaluation are appropriate for the application where the customer intends to use the product. Products then evaluated and validated by NIAP approved laboratories against NSA-certified Protection Profiles or STs will also be noted on NSA's web page.