NCSC-TG-002
Library No. S-228,538
Version 1

# FOREWORD

The National Computer Security Center has established an aggressive program to study and implement computer security technology, and to encourage the widespread availability of trusted computer products for use by any organization desiring better protection of their important data. The Trusted Product Evaluation Program focuses on the security evaluation of commercially produced and supported computer systems by evaluating the technical protection capabilities against the established criteria presented in the Trusted Computer System Evaluation Criteria. This program, and the open and cooperative business relationship being forged with the computer and telecommunications industries, will result in the fulfillment of our country's computer security requirements. We are resolved to meet the challenge of identifying trusted computer products suitable for use in processing sensitive information. A key service of the National Computer Security Center to the computer security community is to act as a clearinghouse for computer security issues and to develop technical security guidelines for automatic data processing systems and networks. This technical information exchange provides guidance and interpretations for the security evaluation process and offers the vendors a central point for technical exchange.

PATRICK R. GALLAGHER, JR. 1 March 1988
DIRECTOR
NATIONAL COMPUTER SECURITY CENTER

# PREFACE

This publication describes procedures for interacting with the National Security Agency's Information Security Organization as related to the Trusted Product Evaluation Program within the National Computer Security Center. It provides the information needed to submit a computer product for technical security evaluation and outlines the National Security Agency's responsibilities for positive, timely acknowledgements. This publication specifically covers the National Computer Security Center's relationship with vendors of proposed trusted computer products from the initial contact with the vendor through the completion of the security evaluation process and follow-on programs. Although more detailed instructions will be referenced in this publication, sufficient guidelines are established for any first-time user of the National Computer Security Center's services. The Office of Industrial Relations invites your comments on this document and on the National Computer Security Center's procedures for conducting security evaluations of computer products. In cooperation with the computer industry, we can improve our national security through the availability of trusted computer products.

## INTRODUCTION

In January 1981 the Director of the National Security Agency was assigned the responsibility for computer security for the Department of Defense. This action led to the formation of the Computer Security Center at the National Security Agency. The Computer Security Center's Charter, promulgated in Department of Defense Directive 5215.1 in October 1982, specifically tasks the Computer Security Center to establish and maintain "... technical standards and criteria for the security evaluation of trusted computer systems that can be incorporated readily into the Department of Defense component life-cycle management process..." The developmental experiments in the 1970's ranged from attempts to add security front-ends to existing systems to designing secure systems and hardware from scratch. Early research and development efforts defined a graduated scale of security features and design principles. These features and principles were incorporated in the Department of Defense Trusted Computer System Evaluation Criteria (Orange Book). The Orange Book was issued in August 1983. In December 1985, the Orange Book was reissued as a Department of Defense Standard (DOD 5200.28-STD). The National Computer Security Center (the Center) responds to a growing need for, and recognizes technical challenges involved in, providing effective protection within computer systems and networks of systems. The Center relies on an open and cooperative relationship with government, industry representatives, and the academic community to accomplish these important objectives. The government encourages industry to provide the computer security capabilities government needs. The Center sponsors critical research, and makes the results widely available to encourage their incorporation into trusted computer products and secure applications. The Center performs security evaluations of computer software and hardware products on commercially or government-produced computer systems. A trusted computer system is defined as a system that employs sufficient hardware and software integrity measures to allow its use to simultaneously process a range of sensitive unclassified or classified (e. g., confidential through top secret) information for a diverse set of users without violating access privileges. Levels of trust are based on the ability of the computer system to enforce access privileges to authorized users and to system protected files. The Center evaluates the security features of trusted products against established technical standards and criteria, and maintains the Evaluated Products List. The Evaluated Products List is a compilation of all computer products which have undergone formal security evaluations, and indicates the relative security merit of each computer product. The criteria against which computer systems are evaluated is the Orange Book. This provides a metric for distinguishing a range of features and assurances for security controls built into automatic data processing system products. The Orange Book establishes specific requirements that a computer system must meet in order to achieve a specific level of trustworthiness. The levels are arranged hierarchically into four major divisions of protection, each with certain security-relevant characteristics. These divisions are subdivided into levels of trust. In recognition of the complex and technical nature of the issues addressed by the Orange Book, the Center has established a Technical Guidelines Program. This program augments information provided in the Orange Book by publishing additional guidance on issues and features addressed therein.

## TRUSTED PRODUCT SECURITY EVALUATION

This section provides the potential computer product vendor with an overview of the Center's Trusted Product Evaluation Program. The process of a trusted product evaluation is illustrated in Figure One. The Pre-Evaluation Review includes the initial contact between the vendor and the National Security Agency, the decision-making process to initiate, and the signing of a Memorandum of Understanding. Note: subsystem products do not require a Memorandum of Understanding but are initiated with a Memorandum of Agreement. The Trusted Product Developmental Process provides the vendor the opportunity to obtain assistance from the Center during the development of a system or network product. The formal product evaluation consists of the actual security evaluation of the vendor's computer system. Successful completion of this process results in the vendor's computer product being placed on the Evaluated Products List.

## PRE-EVALUATION REVIEW

Five milestones in the application process must be reached before the security evaluation of a proposed computer product can begin.

1. Initial Contact
2. Certificate Pertaining to Foreign Interests
3. Proposal Package
4. Program Decision
5. Memorandum of Understanding (Memorandum of Agreement for Subsystems)

## INITIAL CONTACT

The National Security Agency point of contact for the Trusted Product Evaluation Program is the Office of Industrial Relations. Interested companies are encouraged to call or write to:

Director, National Security Agency
Attention: Office of Industrial Relations
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000
(301) 688-6581

## CERTIFICATE PERTAINING TO FOREIGN INTERESTS

Before submitting an application for the Trusted Product Evaluation Program, the Center requires that all companies submit a completed Certificate Pertaining to Foreign Interests prior to undertaking the additional effort to prepare a proposal package. For those companies that already have a facility security clearance, a current DD Form 441s may be sent in lieu of the Certificate Pertaining to Foreign Interests. Please submit the certificate or DD Form 441s to the Office of Industrial Relations, as listed above.

## PROPOSAL PACKAGE

After contact has been established, the vendor must prepare a proposal package in accordance with the following guidance. Four copies of the proposal package are required.

This point cannot be over emphasized; information marked Company Proprietary is protected to the fullest extent permitted under the law, and must be marked accordingly. The product proposal package should demonstrate corporate-level support for the product evaluation effort and consist of a company profile, market information and a written product proposal.

COMPANY PROFILE

Potential computer security product vendors, whether requesting a system, a network, or a subsystem evaluation, must establish a formal working relationship with the Center. Vendors are encouraged to submit as much detailed documentation as necessary to establish their capability and suitability for the Trusted Product Evaluation Program. The company profile portion of the submission shall include at least the following information:

Company name and address.

State of incorporation and composition of ownership.

Principal point of contact, a technical point of contact, and a public point of contact. For each, include name and title, business address, and business telephone. Public point of contact names will be placed on a list that can be provided to any requestor desiring to establish a business connection with your company.

Product or services offered. This could be supplemented with a company capabilities brochure.

A recent annual or certified financial report.

Number of people employed by the company, and in the case of a system or network product, the projected size of the team which will be developing, enhancing and/or maintaining the proposed product.

MARKET INFORMATION

To evaluate the requirements for any proposed product, the vendor must provide sufficient detail to identify the utility in the market place. The information below covers the minimum market information the Center requires to assess the probable need in the community. The market information portion of the proposal package shall identify:

Intended market by product type and level of trust, including a specific customer base and/or firmly established requirements.

Portion of markets intended to address. How the specific market projections were derived. In cases where the product to be developed is a retrofit to existing equipment, include the potential volumne of sales for those existing equipments that are already fielded.

Known or projected U.S. Government requirements that the product will satisfy. Distinguish between DOD and Civil Agency.

Known or projected commercial requirements that the product will satisfy.

WRITTEN PRODUCT PROPOSAL

A separate proposal is required for each computer product submitted for security evaluation. These products must be of direct and obvious benefit to the information security posture of the nation, and should address the applicable requirements outlined in established criteria or interpretations. This determination will be based on the information contained in the product proposal, measured against national computer security needs and priorities.

The Center presently conducts three distinct types of product evaluations: 1) the system evaluation, 2) the network evaluation, and 3) the subsystem evaluation.

Proposals For System Evaluations

The Center evaluates as a system that product which addresses all of the requirements of a given class of the Orange Book.

Although complete information about the proposed product may not be available at this stage of the design, the written product proposal should provide the following information:

Technical description of the product.

What is the targeted class or level of trust?

What is the operating system for your product?

Is the proposed product currently in use? If so, what is the current installed base?

What is the projected installed base over the nextve years?

What is the target development schedule? How flexible is this schedule and by what date do you plan to bring this product to market?

What are the known or projected requirements that the product will satisfy? (Distinguish between the Department of Defense and Civil Agencies.)

What are the differences between and advantages of the proposed product relative to similar products which are currently available?

## Proposals For Network Evaluations

The Center defines a network as everything that is needed to accomplish a job, end user to end user. The Center defines a network component as any part of a network.

The Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria (TNI) is currently the criteria against which networks are evaluated.

Written product proposals should provide the following information:

A technical description of the product.

What is the underlying security policy of the product?

What level of protection is provided by the product?

What is the projected schedule for development?

What are the environments for which the product is intended? Include an overall description of the product. Compare it to another product currently available if possible.

Does your product interact with users directly? If so, does it provide all of the functionality identified at one of the criteria levels in Part I of the TNI, or only a subset?

If it is a network system, what level of trust does it meet according to Part I of the TNI?

If it is a network component, which of the following functionalities does it provide, and at which level of trust is each functionality provided?

Mandatory Access Control

Discretionary Access Control

Identification and Authenication

What other security services mentioned in Part II of the TNI does your product provide?

What type of carrier medium, if any, is used or supported by your product?

## Proposals For Subsystem Evaluations

The Center defines a computer security subsystem as a physical device or software mechanism which is added to a computer system to enhance the computer security functionality of the overall system.

To be considered for a subsystem evaluation, a company must have an existing product which is designed to provide one or more of the following capabilities, as described in the Trusted Computer System Evaluation Criteria:

1) mandatory access control;

2) audit;

3) discretionary access control;

4) identification and authentication; or.

5) object re-use.

Written product proposals should provide the following information:

A technical description of the product.

Which of the five subsystem functionalities does the product implement?

What is the current installed base? What is the projected installed base over the next five years?

What is the current or projected market for your product (to include specific customer base and/or firmly established requirements, if possible)? What portion of this market do you intend to address? How were the specific market projections derived?

What are the known or projected requirements that the product will satisfy? (Distinguish between the Department of Defense and Civil Agencies.)

What are the differences between and advantages of the proposed product relative to similar products which are currently available?

PROGRAM DECISION

Upon receipt of the company's proposal package, the Office of Industrial Relations will send the company written notification that the package has been received and is under consideration. The proposal will be reviewed to determine its value while assessing the capabilities of the company, the utility of the product to the Federal Government, and the degree to which the product addresses the technical aspects of computer security. The availability of adequate Center resources to support the evaluation program is also a prime consideration in the program decision. The Center may need to meet with the vendor's technical experts to ensure decision making processes are based on sound technical understanding of the product. When a decision is reached, the Office of Industrial Relations will notify the vendor in writing whether the product has been accepted for evaluation. System and network evaluations will enter into the Trusted Product Developmental Process as described below. Subsystem evaluations enter directly into the formal evaluation.

## MEMORANDUM OF UNDERSTANDING

If a package for a system or network product is accepted, a Memorandum of Understanding is executed between the vendor and the National Security Agency. The purpose and function of the Memorandum of Understanding is to establish a legal relationship between the National Security Agency and the potential vendor in which:

> The National Security Agency agrees to provide necessary and relevant computer security information and guidance to the potential vendor.
>
> The vendor agrees to provide the National Security Agency the information necessary to assess the security of the proposed product.
>
> The vendor agrees to follow the intent and requirements of the procedures leading to a system, network or subsystem evaluation.
>
> The National Security Agency agrees to protect vendor proprietary information which is provided under the Memorandum of Understanding.
>
> Both parties agree to review the continuation and terms of the Memorandum of Understanding periodically.

A program manager within the Requirements and Resources Division at the Center will be assigned to monitor and coordinate technical and/or administrative responses to the vendor, and a technical point of contact within the Product Evaluation Division will be identified to the vendor. To determine the division and class at which all requirements are met by a computer system, the system must be evaluated against the Orange Book. This security evaluation will be conducted by a Center evaluation team.

## TRUSTED PRODUCT DEVELOPMENTAL PROCESS

The primary thrust of this phase is an in-depth examination of a vendor's design either for a new trusted product (system or network) or for security enhancements to an existing product.It is intended to ensure that the product is actually ready for evaluation with all necessary evidence available so the evaluation can be completed without delays for additional development or evidence generation. This phase is based primarily on design documentation and information supplied by the vendor, and it involves little or no "hands on" use of the product.

This phase results in the production of an Initial Product Assessment Report.

This report documents the evaluation team's understanding of the system based on the information presented by the vendor, and assigns a candidate Orange Book class rating to the system. The candidate rating is an estimate of the highest class for which the product has displayed some evidence for each of the requirements in the Orange Book.

The Center's Technical Review Board provides a consistency check on the application of the Orange Book requirements, and ensures the product is ready for evaluation. Because the Initial Product Assessment Report does not represent a complete analysis of the computer product and may contain proprietary information, distribution is restricted to the respective vendor and the Center.

## SYSTEM AND NETWORK FORMAL EVALUATIONS

To enter this formal evaluation phase, the design of a computer system must be finalized and marketable. In addition, the product release being evaluated must not undergo any additional development. Once the product is accepted for evaluation, a Memorandum of Agreement is signed between the Center and the vendor, to address the formal aspects of the product receiving an Evaluated Products List rating and the accompanying responsibilities.

At the start of this phase, a Product Bulletin is released by the enter announcing the evaluation. The Product Bulletin is a brief description of the computer system undergoing security evaluation, and includes the candidate rating of the system.

The evaluation phase is a detailed analysis of the hardware and software components of a system, all system documentation, and a mapping of the security features and assurances to the Orange Book. The analysis performed during this phase requires "hands on" testing (i.e., functional testing and, if applicable, penetration testing).

The evaluation phase leads to the Center publishing a Final Evaluation Report and an Evaluated Products List entry. The Final Evaluation Report is a summary of the security evaluation and includes the Evaluated Products List rating, which is the final class at which the product successfully met all Orange Book requirements in terms of both security features and assurances. The Final Evaluation Report and the Evaluated Products List entry are made public. The evaluation process represents a firm commitment from the vendor, and at its completion the product will receive a rating from the Center.

## SUBSYSTEM FORMAL EVALUATIONS

While the Center devotes much of its resources to encouraging the production and use of multipurpose trusted computer systems, there is a recognized need for guidance on, and security evaluation of, supplementary computer security products. These subsystems may not meet all of the security feature, architecture, or assurance requirements of any one security class or level of the Orange Book. To meet this need, the Center has established the subsystem evaluation process.

The goal of the Center's subsystem evaluations is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements in existing installations. Once a subsystem product is accepted for evaluation, a Memorandum of Agreement is signed between the Center and the vendor, addressing the formal aspects of the product being included in the Evaluated Products List and the accompanying responsibilities.

Subsystems are special-purpose products which can be added to existing computer systems to increase some aspect of security and have the potential of meeting automatic data processing security needs. For the most part, the scope of a subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment or computer system on which the subsystem may be implemented. To promote consistency in evaluations, an attempt is made to assess a subsystem's security-relevant performance in light of applicable standards and features outlined in the Orange Book. In addition, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the computer product performs as advertised. Upon completion, a summary of the Final Evaluation Report will be placed on the Evaluated Products List.

The Final Evaluation Report will not assign a specific rating to the computer product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security. The Final Evaluation Report and the Evaluated Products List entry are made public.

EVALUATED PRODUCTS LIST

The Evaluated Products List provides computer users, managers and security officials, an authoritative and unbiased security evaluation of a computer system's suitability for use in processing classified and sensitive information. All products on the Evaluated Products List have been evaluated against the established criteria and interpretations. A Final Evaluation Report is issued for all products. The rating given to a system product is the highest class for which all the requirements in the Orange Book have been met. Trusted product security evaluation results are published in formal reports available from either the Government Printing Office or the National Technical Information Service.

The overall evaluation class ratings given in the Evaluated Products List apply only to the specific hardware/software configurations listed. As such, the rating indicates that the product met or exceeded each of the individual requirements for the overall Evaluation Class. Although the computer product was subjected to the detailed security testing specified in the Orange Book, it must be emphasized that such testing is not sufficient to guarantee the absence of flaws in the product. The Evaluated Products List entry does not constitute a general or overall endorsement of the product by the government, nor does it constitute a Department of Defense certification or accreditation of the trusted computer product for use in classified or sensitive unclassified processing environments. Rather, the security evaluation provides an essential part of the technical evidence required for follow on certification and accreditation. Ultimate responsibility for the continuing integrity provided by the security mechanisms of any trusted computer product evaluated by the Center rests solely with the vendor. The Evaluated Products List, which documents evaluated computer products, is available to vendors to actively market and advertise the overall evaluation class rating achieved by their products to procurement authorities and the general public.

The Evaluated Products List contains entries for general-purpose operating systems, add-on packages, and subsystems. Product Bulletins, which are synopses of computer systems currently undergoing formal security evaluations by the Center, are also included on the Evaluated Products List.

A hard copy of the Evaluated Products List is included in the Information Systems Security Products and Services Catalogue. This catalogue is updated quarterly and is available through the Government Printing Office.

## RATINGS MAINTENANCE PHASE

The Ratings Maintenance Phase provides a mechanism to ensure the validity of a previous rating for a new version of an evaluated computer system product. As enhancements are made to the computer product the Ratings Maintenance Phase ensures that the level of trust is not degraded. A complete re-evaluation is required to achieve a higher rating.

The Ratings Maintenance Phase is designed to keep the Evaluated Products List current. This is accomplished by using the personnel involved in the maintenance of the product to manage the change process and reduce the effort required to extend the rating.

Success of the Ratings Maintenance Phase depends upon the development of a cadre of vendor personnel with a strong technical knowledge of computer security and of their computer product. These trained personnel will oversee the vendor's computer product modification process. They will certify to the Center that any modifications or enhancements applied to the product will preserve the security mechanisms and maintan the assurances.

The Ratings Maintenance Phase is initially designed for C1 - B1 level of trust systems. As experience is gained in the program, the intent is to extend to higher level systems and to networks.

## EVALUATION SUPPORT SERVICES

The Center supports the trusted product security evaluation process within the Trusted Product Evaluation Program. The following specialized technical services are available to benefit the interactive relationship between the computer product vendors and the technical staff of the Center. To obtain these services or to gain more insight into their particular detail, refer to the Points of Contact section.

### DOCKMASTER

DOCKMASTER is an unclassified computer system used by the Center for the nationwide dissemination and exchange of computer security information. DOCKMASTER serves the entire information security community including the Federal Government, universities, and private industry. It can distribute electronic mail via connections to the ARPANET. DOCKMASTER is accessible by direct dial, the MILNET, and McDonnell Douglas Tymnet network.

DOCKMASTER is the primary means of communications between the vendor and the Center throughout the computer product security evaluation process. It allows vendors to use electronic mail, file transfer protocols, and the Forum subsystem. Forum is an on-line, interactive meeting facility that permits an individual to "meet" with other users through the use of a computer terminal.

## VERIFICATION TOOLS

Vendors who are developing systems that are targeted to meet the class A1 requirements of the Orange Book must provide assurance that the system implementation is consistent with the system's design. This assurance is gained by developing a Formal Top Level Specification of the design and verifying that the specifications are consistent with the formal security policy model (the security requirements) for the system. After the design verification has been completed, an informal mapping is performed from the Formal Top Level Specification to the implementation. This completes the evidence. Formal Top Level Specification development and subsequent verification is a rigorous, mathematical process that can be greatly aided by the use of automated verification tools. The Orange Book requires the use of such a tool in the verification of A1 systems: "This verification evidence shall be consistent with that provided within the state-of-the-art of the particular Center endorsed formal specification and verification system used."

The Center endorsed verification tools are maintained on the Endorsed Tools List. Examples of these verification tools are Formal Development Methodology, Gypsy, and Enhanced Hierarchical Development Methodology. For information concerning the current entries on the Endorsed Tools List, vendors should contact the Computer Hardware and Software Support Division.

## TECHNICAL GUIDELINES

To complement the information contained in the Orange Book, the Center publishes technical guidelines which serve as additional guidance in interpreting the established standard. These technical guidelines aid in the evaluation and selection of computer security products, both complete systems and subsystems. In addition, they are used throughout the Federal Government and by Federal Government contractors as guidance for the procurement, use, and disposal of automation systems and their associated magnetic storage media.

The Technical Guidelines Program contributes to the technical literature on issues of computer security. Guidelines are written in response to demonstrated need in automated processing environments.

Participation in the development of technical guidelines is provided by the technical staff of the Center and its associated offices within the National Security Agency, by representatives of the Department of Defense and the Intelligence Community, by civil agencies of the Federal Government, by Federally Funded Research and Development Centers, by contracted analytic and technical firms, and by selected experts in the particular field of endeavor. Draft versions of proposed documents are extensively reviewed by a wide audience of interests, and comments are fielded for consideration before publication.

PUBLICATIONS

Technical guidelines that are published by the Center, and useful to a vendor in order to process a computer product through the Trusted Product Evaluation Program, will be provided in limited quantity by the INFOSEC Awareness Organization.

TRAINING

The Center provides training on topics of major importance to vendors interested in the trusted product security evaluation process.

OTHER RELATED SERVICES

Within the Information Security Organization, there are several separate but complementary programs which relate to the Trusted Product Evaluation Program. A brief description of each program is provided in subsequent paragraphs. For more details, please contact the specific program office in the Points of Contact list.

Like the Trusted Product Evaluation Program, the Commercial Communications Security Endorsement Program is a business relationship which combines private sector leadership and expertise in equipment design, development and high volume production with the information security expertise of the National Security Agency. Specifically, this program is designed to encourage industry to embed United States Government proprietary cryptography into telecommunications products to meet the need to protect its classified and sensitive unclassified information. The Commercial Communications Security Endorsement Program products that are endorsed for protecting sensitive unclassified government information only are also available to the private sector. In today's computer networking environment, many products require both an encryption capability and a trusted computing base to meet user requirements. Companies whose products merge both communications and computer security disciplines are encouraged to become familiar with the requirements of the Commercial Communications Security Endorsement Program.

The Secure Data Network System Program was established in August 1986, when the National Security Agency joined in partnership with ten major telecommunications and computer companies to develop a security architecture and a user-friendly key management system using the Open Systems

Interconnection model. The ultimate goal of the Secure Data Network System Program is to provide for the development of information security products that can operate over a broad range of commercial data networks. Once the Secure Data Network System architecture is formalized, the development of Secure Data Network System products will be carried out under the auspices of the Commercial Communications Security Endorsement Program.

The Industrial TEMPEST Program is designed to aid industry in developing and testing TEMPEST-suppressed equipment which can be offered for sale to the United States Government. Companies developing trusted computing products should be aware that the United States Government may require that products protecting classified information be TEMPEST-suppressed.

A company that produces computer security products may be interested in the Department of Treasury's Electronic Funds Transfer Certification Program if the primary function of its product is to provide message authentication in support of United States Government financial transactions. The program specifically provides for testing, evaluating and certifying Message Authentication Code devices for Federal electronic funds transfer use in accordance with American National Standards Institute Standard X9.9. In addition, elements of Federal Standard 1027 covering minimum general security requirements for implementing the Data Encryption Standard encryption algorithm are included. Optional electronic key management is based on American National Standards Institute Standard X9.17.

Vendors who are developing trusted computer products as Independent Research and Development Projects may obtain technical assistance and technical plan evaluations by contacting the Center's Office of Computer Security Research and Development.

The Computer Security Technical Vulnerability Reporting Program, promulgated in Department of Defense Instruction 5215.2 in September 1986, provides a mechanism for reporting weaknesses or design deficiencies in hardware, firmware, or software that leave automated information systems open to potential exploitation. Technical vulnerabilities reported in Evaluated Products List items could possibly change the overall rating of the product.

## Points of Contact

COMMERCIAL COMMUNICATIONS SECURITY ENDORSEMENT PROGRAM

Director, National Security Agency
Attention: Office of Industrial Relations
9800 Savage Road
Fort George G.Meade, MD 20755-6000
(301) 688-6581

TRUSTED PRODUCT EVALUATION PROGRAM

Director,National Security Agency
Attention: Office of Industrial Relations
9800 Savage Road
Fort George G.Meade, MD 20755-6000
(301) 688-6581

COMPUTER SECURITY TECHNICAL VULNERABILITY REPORTING PROGRAM

Director,National Security Agency
Attention: Vulnerability Reporting Program
9800 Savage Road
Fort George G. Meade, MD 20755-6000
(301) 688-6079

DEPARTMENT OF TREASURY'S ELECTRONIC FUNDS TRANSFER CERTIFICATION PROGRAM

Assistant Director, Security Programs
Department of Treasury
15th and Pennsylvania Avenue NW
Washington, DC 20220
(202) 566-5152

DOCKMASTER AND VERIFICATION TOOLS

National Computer Security Center
Attention: Computer Hardware and Software Support Division
9800 Savage Road
Fort George G. Meade, MD 20755-6000
(301) 859-4360

INDEPENDENT RESEARCH AND DEVELOPMENT PROJECTS PROGRAM

National Computer Security Center
Attention: Office of Computer Security Research and Development
9800 Savage Road
Fort George G.Meade, MD 20755-6000
(301) 859-4486

INDUSTRIAL TEMPEST PROGRAM

Ford Aerospace and Communications Corporation
Attention: Mail Stop 3 (Industrial TEMPEST Program)
7170 Standard Drive

Hanover, MD 21076
(301) 796-5254

PUBLICATIONS AND TRAINING

Superintendent of Documents
U.S. Government Printing Office
ashington, DC 20402
(202) 783-3238

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
(703) 487-4650

SECURE DATA NETWORK SYSTEM PROGRAM

Director, National Security Agency
Attention: Secure Data Network Systems SPO
9800 Savage Road
Fort George G. Meade, MD 20755-6000
(301)668-7110

TECHNICAL GUIDELINES

National Computer Security Center
Attention: Technical Guidelines Division
9800 Savage Road
Fort George G. Meade, MD 20755-6000

## REFERENCES


DoD 3204.1, Independent Research and Development, Under Secretary of Defense for Research and Engineering, 1 December 1983.

DoD Directive 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems, revised April 1978.

DoD 5200.28-STD, Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 1985; supersedes CSC-STD-001, dated 15 August 1983.

DoD Directive 5215.1, Computer Security Evaluation Center, 25 October 1982.

DoD Instruction 5215.2, Computer Security Technical Vulnerability Reporting Program, 2 September 1986.

National Telecommunications and Information System Security Policy No. 200, National Policy on Controlled Access Protection Policy, 15 July 1987.

NCSC-TG-005 Version 1, Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria, 31 July 1987.

# ATTACHMENT I

## SPECIFICATIONS AND DESIGN DOCUMENTATION

When a vendor enters into a product evaluation, he must present evidence that his system and its design meets the appropriate criteria requirements. Examples of the type of evidence normally submitted to support an evaluation include the design specifications that explain the security mechanisms, the Trusted Computing Base (TCB) arguments that show how the TCB is tamperproof, always invoked and small enough to be analyzed. Also, the model (or philosophy of protection) and how it relates to the implementation are important parts of the evidence. The best test of evidence is that it must include all the information such that a new team that is basically unfamiliar with the product could evaluate only the evidence and reach the proper conclusion.

In order for the evaluation team to review this evidence and determine whether the system complies with these requirements, the team must develop a conceptual understanding of how the system being evaluated operates. Generally, the evaluation team can acquire this level of understanding by reviewing the vendor's system documentation and specifications. The following types of high level system documents are typically required by the evaluation team:

User-Level Documentation

Provides users an overview of the system, its functioning, and information on user services.

Operational Manuals

Contains general description,implementation and usage information for the system. It is intended for use by system programmers who service the system.

Program Logic Manuals

Documents the internal operation and organization of a system. It is intended for use by system programmers for program maintenance and to determine the location of program malfunctions.

Administrative Manuals

Documents the procedures for installing and generating the system.

Hardware and Software System Specifications

Includes Hardware and Software design and implementation details of the system major components

ATTACHMENT II

TEST PLANNING

The Department of Defense Trusted Computer System Evaluation Criteria (Orange Book) requires that vendors provide a document to the evaluators that describes the test plan, test procedures, and the results of the security mechanisms functional testing.  Security mechanisms are those mechanisms that are relevant to the Orange Book.  These include object reuse, labeling, discretionary access control (DAC), mandatory access control (MAC), identification and authentication, auditing, and trusted path.  A security related functional test plan should determine whether the system being evaluated has any design and implementation flaws that would permit a subject external to the Trusted Computing Base (TCB) to read, change, or delete data which he would not normally have access to under the mandatory or discretionary security policy enforced by the TCB.  [The TCB is defined by the TCSEC as "the totality of protection mechanisms within a computer system -- including hardware, firmware, and software --the combination of which is responsible for enforcing a security policy"].  Security related functional tests involve all security properties of a system (i.e., all aspect of the TCB that affect or can be affected by a security mechanism).

COVERAGE OF TESTING

Although many standard testing methods are acceptable in fulfilling the Orange Book testing requirements, they are, for all but very small or simplistic systems, impractical to use due to the large amount of resources required. Some methods of testing that have in the past proven to be sufficient and were reasonable to implement are Interface and Mechanism testing.

Interface testing refers to testing the TCB at the user interface (i.e., user callable routines).  Generally, critical boundaries of each security mechanism are determined and test cases on both sides of these boundaries are generated. The critical boundary of a security mechanism is the point at which the rule it is designed to implement is or is not invoked.  This provides more assurance that the view of the system presented to a user is correct.

Mechanism testing refers to the testing of the security mechanisms that the TCB supports (i.e., DAC , object reuse, audit, etc.).  Mechanism can consist of one or more interface, and some interfaces can be called by different mechanisms.  Mechanism testing shows that the TCB supports these mechanisms. The sufficiency of the different methods of testing are dependent on the particular class of the Orange Book the system is being evaluated against.

TESTING A B2-A1 SYSTEM:

TCB interface testing is sufficient.  Every interface must be tested.  Since B2, B3 or A1 systems are well structured, and their Detailed Top Level Specifications (DTLS) and Formal Top Level Specifications (FTLS) provide a complete and accurate description of the TCB interface, the testing of the TCB interfaces can reasonably be expected to be very comprehensive.

TESTING A C1–B1 SYSTEM:

Mechanism testing is probably sufficient. The structure allowed by a C1–B1 architecture would most likely make interface testing impractical. It is likely that an evaluation team may determine, through inspection of the system's test plan and its architecture, that black box testing of the interface is insufficient and requires "white box" testing of instrumental code sections.

DOCUMENTATION

Documentation of a test should be specific and briefly describe the TCB mechanism being tested. The expected results of each test case should be set forth. The test documentation should also contain an overview of the test methods being used, and the security properties which are and are not pertinent for each particular mechanism. A list of all assumptions being made about the testing environment should also be included .

The Orange Book functional testing requirements also require that both the system and the test plan be maintained using good configuration management techniques. This allows the vendor to provide a form of Life–cycle assurances for the system. Life–cycle assurance is a procedure for managing system design, development, and maintenance using a method of rigorous and formalized controls and standards. It allows the vendor to reevaluate the system when changes are made to determine whether the integrity of the protection mechanism has been affected

ATTACHMENT III

REQUIRED DOCUMENTATION

The Orange Book requires that a vendor produce documentation which describes the system protection mechanisms, how the system can operate using these protection mechanisms, how the system developer designed security into the system, and how these security features and system were tested. The amount of documentation required increases with the targeted Orange Book class. The specific requirements are listed below starting at the lower Orange Book classes and progressing through the higher classes. In some cases, additional documentation may be required

C1 - DISCRETIONARY ACCESS CONTROL

Security Features User's Guide tells users how to use the security mechanisms of the system. It provides the necessary information to understand and effectively use the discretionary access control mechanisms to protect information.

Trusted Facility Manual tells the system administrator how to set the system up so that it stays secure. It should tell the administrator how to select the proper options such that the system is operated in a mode that meets the requirements of the Criteria. If there are unsecure modes that the system can run in, the manual should clearly state their impact on the security and include warnings as appropriate. This manual should also include any procedures the administrator should use during operations to maintain security. If any of the hardware/software features require administrator actions to complete the security protection, they should be thoroughly described.

Test Documentation describes results of security mechanism's functional testing. This documentation is used by the evaluation team to assess the testing performed by the vendor. This document describes those tests, how they are run, and how to properly interpret the results.

Design documentation provides the rationale and supporting evidence for the security of the design of the system. The descriptive specifications are included in this evidence. It is intended to provide the sort of information a new developer would need in order to support the system. It should include the manufacturer's philosophy of protection. If the TCB consists of distinct modules, the design documentation describes the interfaces between these modules.

C2 - CONTROLLED ACCESS PROTECTION

Security Features User's Guide remains the same as C1.

Trusted Facility Manual is the same as C1, but also requires details on how to maintain audit data.

Test Documentation remains the same as C1.

Design Documentation is the same as C1.

B1 - MANDATORY PROTECTION

Security Features User's Guide remains the same as C2., but also describes the additional security mechanisms required at this class (i.e., Mandatory Access Control).

Trusted Facility Manual remains the same as C2, but also describes the operator and administrator functions related to security. This includes an explanation of what's involved in changing the security characteristics of a user, and a description of facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner.

Test Documentation remains the same as C2.

Design Documentation remains the same as C2, but also describes the security policy model (either formally, i.e., mathematically, or informally, i.e., in English) and how the TCB implements this model.

B2 - STRUCTURED PROTECTION

Security Features User's Guide remains the same as B1, but also describes the additional security mechanisms required by this class (i.e., Trusted Path).

Trusted Facility Manual remains the same as B1, but also details what constitutes the TCB and how it can be modified. It also describes how separate operator and administrator functions need to be supported.

Test Documentation remains the same as B1, but includes the results of covert channel tests. Covert channels are communication paths that allow a process to transfer information in a manner that violates the system's security policy.

Design Documentation remains the same as B1, but also includes a formal description of the model, and proof that it is sufficient for the policy. It will also describe how the TCB implements the reference monitor concept and how it enforces the principle of least privilege.

B3 - SECURITY DOMAINS

Security Features User's Guide remains the same as B2, but also describes the additional security mechanisms required at this class .

Trusted Facility Manual remains the same as B2, but also includes a description on how to start up and restore the system security. It also describes the role of the Security Administrator.

Test Documentation remains the same as B2.

Design Documentation remains the same as B2, but also includes the correspondence between the Detailed Top Level Specifications and the TCB. The TCB implementation is also shown to be informally consistent with the Detailed

Top Level Specifications.

A1 - VERIFIED PROTECTION

Security Features Users's Guide remains the same as B3.

Trusted Facility Manual remains the same as B3.

Test Documentation remains the same as B3, but also includes the results of the mapping between the Formal Top Level Specifications and the TCB source code.

Design Documentation remains the same as B3, but also includes a description of the components that are strictly internal to the TCB. It also includes a Formal Top Level Specification to TCB correspondence.