The Interpreted TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA Requirements

NATIONAL

COMPUTER SECURITY CENTER

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

12 January 1995

Report No. TBD
C-Evaluation Report No.
Library No. TBD

This page intentionally left blank

FOREWORD

This publication, the **Interpreted TCSEC Requirements** is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document all formal interpretations of the requirements of the **Department of Defense Trusted Computer System Evaluation Criteria**, dated December 1985.

Approved:

Patrick R. Gallagher, Jr.
Director,
National Computer Security Center

12 January 1995

This page intentionally left blank

TABLE OF CONTENTS

FOREWORD **iii**

1 Introduction **1**
1.1 Interpretation Administration . . . 2

2 Criteria Interpretations **3**
2.1 Audit . . . 3
I-0004 Enforcement of audit settings consistent with protection goals . . . 4
I-0005 Action for audit log overflow . . . 4
I-0006 Audit of user-id for invalid login . . . 4
I-0043 Auditing use of unnamed pipe . . . 5
I-0073 OK to audit decision regardless of whether action completed . . . 5
I-0084 Audit least disruptive action . . . 5
I-0172 Audit of imminent security violations . . . 6
I-0286 Auditing unadvertised TCB interfaces . . . 6
2.2 Configuration Management . . . 7
I-0285 CM comparison source or object? . . . 7
2.3 Covert Channel Analysis . . . 8
2.4 Design Documentation . . . 9
I-0192 Interface manuals as design documentation . . . 9
I-0193 Standard system books as design documentation . . . 10
2.5 Design Specification and Verification . . . 11
I-0254 UNIX-style manual pages as DTLS . . . 11
2.6 Device Labels . . . 12
I-0007 Assigning device level range . . . 12
2.7 Discretionary Access Control . . . 13
I-0002 Delayed revocation of DAC access . . . 13
I-0020 DAC authority for assignment . . . 14
I-0053 Public objects and DAC . . . 14
I-0222 Passwords not acceptable for DAC . . . 14
I-0312 Set-ID and the DAC requirement . . . 14
2.8 Exportation of Labeled Information . . . 16
2.9 Exportation to Multilevel Devices . . . 17
2.10 Exportation to Single-Level Devices . . . 18
2.11 Identification and Authentication . . . 19
I-0001 Delayed enforcement of authorization change . . . 19
I-0096 Blanking passwords . . . 19
I-0240 Passwords may be used for card input . . . 20
I-0288 Actions allowed before I&A . . . 20
2.12 Label Integrity . . . 21
2.13 Labeling Human-Readable Output . . . 22
I-0022 One set of banner pages around multiple outputs . . . 22
I-0039 Multilevel printers and page labeling . . . 22

I-0040 Requirements for overwrite label capability . . . 23
I-0253 Default page marking format . . . 23
I-0275 Single-level printers and page labeling . . . 23
2.14 Labels . . . 25
2.15 Mandatory Access Control . . . 26
I-0003 Access validation after object label change . . . 26
I-0239 Subject access revocation after change in user clearance . . . 27
2.16 Object Reuse . . . 28
I-0041 Object reuse applies to all system resources . . . 28
2.17 Security Features User's Guide . . . 29
I-0244 Flexibility in packaging SFUG . . . 29
2.18 Security Testing . . . 30
I-0170 Functional tests required for object reuse . . . 30
2.19 Subject Sensitivity Labels . . . 31
2.20 System Architecture . . . 32
I-0213 Administrator interface is part of TCB . . . 32
2.21 System Integrity . . . 33
I-0144 Availability of diagnostics . . . 33
2.22 Test Documentation . . . 34
2.23 Trusted Distribution . . . 35
2.24 Trusted Facility Management . . . 36
I-0315 Restricted to trusted administrative interface . . . 36
2.25 Trusted Facility Manual . . . 37
I-0046 Detailed audit record structure . . . 37
I-0069 Flexibility in packaging TFM . . . 37
2.26 Trusted Path . . . 39
2.27 Trusted Recovery . . . 40

3 Interpretation Rationale **41**
I-0001 Delayed enforcement of authorization change . . . 41
I-0002 Delayed revocation of DAC access . . . 42
I-0003 Access validation after object label change . . . 43
I-0004 Enforcement of audit settings consistent with protection goals . . . 45
I-0005 Action for audit log overflow . . . 45
I-0006 Audit of user-id for invalid login . . . 46
I-0007 Assigning device level range . . . 47
I-0020 DAC authority for assignment . . . 47
I-0022 One set of banner pages around multiple outputs . . . 48
I-0039 Multilevel printers and page labeling . . . 49
I-0040 Requirements for overwrite label capability . . . 50
I-0041 Object reuse applies to all system resources . . . 50
I-0043 Auditing use of unnamed pipe . . . 51
I-0046 Detailed audit record structure . . . 52
I-0053 Public objects and DAC . . . 53
I-0069 Flexibility in packaging TFM . . . 53
I-0073 OK to audit decision regardless of whether action completed . . . 54
I-0084 Audit least disruptive action . . . 54
I-0096 Blanking passwords . . . 55

I-0144 Availability of diagnostics . . . 56
I-0170 Functional tests required for object reuse . . . 56
I-0172 Audit of imminent security violations . . . 57
I-0192 Interface manuals as design documentation . . . 57
I-0193 Standard system books as design documentation . . . 58
I-0213 Administrator interface is part of TCB . . . 59
I-0222 Passwords not acceptable for DAC . . . 60
I-0239 Subject access revocation after change in user clearance . . . 60
I-0240 Passwords may be used for card input . . . 61
I-0244 Flexibility in packaging SFUG . . . 62
I-0253 Default page marking format . . . 62
I-0254 UNIX-style manual pages as DTLS . . . 63
I-0275 Single-level printers and page labeling . . . 64
I-0285 CM comparison source or object? . . . 65
I-0286 Auditing unadvertised TCB interfaces . . . 66
I-0288 Actions allowed before I&A . . . 66
I-0312 Set-ID and the DAC requirement . . . 67
I-0315 Restricted to trusted administrative interface . . . 67

A Previous Interpretations **69**
Security Testing - Interpretation (Report No. C1-CI-01-83) . . . 69
Identification and Authentication - Interpretation (Report No. C1-CI-02-83) . . . 70
Audit - Interpretation (Report No. C1-CI-01-84) . . . 72
Security Testing - Interpretation (Report No. C1-CI-02-84) . . . 73
Audit - Interpretation (Report No. C1-CI-04-84) . . . 75
Exportation to Multilevel Devices - Interpretation (Report No. C1-CI-05-84) . . . 76
Discretionary Access Control - Interpretation (Report No. C1-CI-06-84) . . . 78
Audit - Interpretation (Report No. C1-CI-07-84) . . . 79
Device Labels - Interpretation (Report No. C1-CI-01-85) . . . 81
Audit - Interpretation (Report No. C1-CI-02-85) . . . 82
Discretionary Access Control - Interpretation (Report No. C1-CI-03-85) . . . 83
DAC by Default - Interpretation (Report No. C1-CI-03-86) . . . 85
Server - Interpretation (Report No. C1-CI-02-86) . . . 86
Operator Log-on - Interpretation (Report No. C1-CI-04-86) . . . 88
System Architecture - Interpretation (Report No. C1-CI-04-85) . . . 90
Discretionary Access Control - Interpretation (Report No. C1-CI-01-86) . . . 92
FTLS Accuracy - Interpretation (Report No. C1-CI-01-87) . . . 93
Audit - Interpretation (Report No. C1-CI-02-87) . . . 95
Exportation of Labels-Interpretation (Report No. C1-CI-01-88) . . . 97
Audit Interpretation (Report No. C1-CI-01-89) . . . 98
Audit Interpretation (Report No. C1-CI-02-89) . . . 99
DAC Public Objects Interpretation (Report No. C1-CI-03-89) . . . 101

B Chronological Interpretation Summary **103**

C Interpretation Working Group Charter **105**
Input Sources . . . 105
Review and Approval Process . . . 106

Outputs 106

D Acronyms **109**

E Bibliography and References **111**

Chapter 1
Introduction

This document has been created to provide clarification of the requirements as stated in the *Trusted Computer System Evaluation Criteria* (TCSEC)[1]. The TCSEC was created many years ago and attempted to, in most cases, provide general statements of security related criteria. But in its years of application, evaluators and users have found that the types of systems being evaluated have evolved from the example systems the TCSEC was based on (e.g., from mainframes to workstations), the general criteria are sometimes difficult to apply to a specific situation, and, occasionally, criteria are missing or not correct. To improve this situation, the National Security Agency (NSA) produces interpretations of the TCSEC. Some major interpretations are for technology that was not sufficiently addressed in the TCSEC such as networks (*Trusted Network Interpretation* (TNI)[3]), and database management systems (*Trusted Database Management System Interpretation* (TDI)[2]). This document, by contrast, contains interpretations resulting from specific questions raised during evaluations, and attempts to build a body of "case law" by addressing system-specific clarifications rather than providing general, all-encompassing interpretations.

These interpretations are not the first attempt to create interpretations for the TCSEC. In fact, this effort is merely a continuation of the effort that started soon after the NSA began evaluating systems. The first interpretation efforts tried to find a general, complete answer to each issue. After handling some of the easy topics, it was found that general purpose interpretations were often impossible to find for difficult topics. The process of generating interpretations ground to a halt. Those first interpretations may be found in Appendix A, page 69, as well as on the Eval_Announcements forum on Dockmaster in their original form. They also were not in a consistent format and it was difficult to find all the ones affecting a particular requirement at a particular level. Therefore, those interpretations, after being updated, are being integrated into this document.

The guiding force producing these interpretations is the NSA's Interpretations Working Group (IWG). The IWG identifies issues; generates draft interpretations; provides them for review by the evaluation, vendor and other computer security people on the Criteria_Discussion forum on Dockmaster; updates them until a sufficient consensus is reached; and then formats them for management review before publishing them in this document. Aside from the old interpretations, issues needing interpretation are raised on the internal evaluator technical discussion forums, on the vendor discussion forums, and as a result of Technical Review Board (TRB) actions. The IWG tries to make an initial response to evaluation team and vendor generated issues and then adds each issue to a database of issues needing interpretation. From this database issues are chosen to go through the full interpretation process.

To provide a ready reference to these interpretations, this document packages them with the requirements to which they apply, using the TCSEC Appendix D, *Requirement Directory*, format. First the criteria and applicable interpretations are presented by requirement and then the interpretation rationale is presented by interpretation number.

1.1 Interpretation Administration

Each interpretation will be announced (i.e., posted) on the Eval_Announcements forum as it is approved by the NSA. Subsequently, a new version of this report will be generated, including the new interpretation, and made electronically available on Dockmaster, in PostScript format. It will be located at the following path name:

> *>udd>CPE>public>iwg>Interpreted.TCSEC.*YY-MM-DD*.ps.*

Note that "YY-MM-DD" represents the date of publication and only the most recent version will be kept available. Additionally, a hardcopy version of this report will be published annually.

Interpretations will be effective when announced. However, they will be enforced only if one of the following conditions is met:

- if approved prior to the formal evaluation phase (under the old evaluation process),
- if approved prior to evaluation (i.e., a successful IPTR, under the new evaluation process),
- if approved more than one year before the current RAMP action (i.e., the RAMP TRB date), or
- if approved before the previous RAMP action.

Appendix B, page 103, provides a list of interpretations, ordered by date, accompanied by the applicable levels of trust. This list should help to quickly identify which interpretations may apply to a particular version of a particular product.

Chapter 2
Criteria Interpretations

This chapter lists requirements defined in **Department of Defense Trusted Computer System Evaluation Criteria** alphabetically rather than by class. For each requirement, three types of criteria may be present, in addition to the list of any relevant interpretations. Each criteria type will be preceded by the word: *NEW*, *CHANGE*, or *ADD* to indicate the following:

NEW: Any criteria appearing in a lower class are superseded by the criteria that follow.

CHANGE: The criteria that follow have appeared in a lower class but are changed for this class. Highlighting is used to indicate the specific changes to previously stated criteria.

ADD: The criteria that follow have not been required for any lower class, and are added in this class to the previously stated criteria for this requirement.

The criteria of each requirement are followed by the statements of all applicable interpretations.

2.1 Audit

C1: *NO REQUIREMENT.*

C2: *NEW:* The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

B1: *CHANGE:* For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object **and the object's security level**. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity **and/or object security level**.

ADD: The TCB shall also be able to audit any override of human-readable output markings.

B2: *ADD:* The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels.

B3: *ADD:* The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded, and, if the occurrence or accumulation of these security relevant events continues, the system shall take the lease disruptive action to terminate the event.

A1: *NO ADDITIONAL REQUIREMENT.*

I-0004 Enforcement of audit settings consistent with protection goals

This interpretation is effective 1993-10-20 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirement that "The ADP system administrator shall be able to selectively audit ..."

> If the TCB supports the selection of events to be audited, it shall provide a method for immediate enforcement of a change in audit settings (e.g., to audit a specified user, to audit objects at a particular sensitivity level); however, the immediate method (e.g., shutting the system down) need not be the usual method for enforcement. The TFM shall describe both the usual enforcement of audit settings and, if the immediate enforcement method is different from the usual one, how an administrator can cause immediate enforcement.
>
> The TFM shall describe the consequences of changing an audit state dynamically if such changes could result in incomplete or misleading audit data.

I-0005 Action for audit log overflow

This interpretation is effective 1993-10-20 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall be able to create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects."

> When the TCB becomes unable to collect audit data, it shall give a clear indication of this condition and take a pre-specified action. The system implementation may allow an administrator to choose from a range of actions. One of the actions that may be chosen by the administrator (or, if no choice is possible, the only action) shall be that the system cease performing auditable events when the TCB is unable to collect audit data. Choosing an audit overflow action shall be considered a security-relevant administrative event for the purposes of auditing. The TFM shall fully describe the administrator's options.

I-0006 Audit of user-id for invalid login

This interpretation is effective 1993-10-20 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, ... For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event."

> While the audit mechanism is required to be capable of producing a record of each login attempt, on failed login attempts it is not required to record in the audit record the character string supplied as the user identity.

I-0043 Auditing use of unnamed pipe

This interpretation is effective 1994-04-19 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirements that "The TCB shall be able to record the following types of events: ... introduction of objects into a user's address space (e.g., file open, program initiation), ... For events that introduce an object into a user's address space..."

> In products that support mechanisms similar to unnamed pipes in UNIX systems, the creation of an unnamed pipe shall be auditable; however, the auditing may be delayed until the pipe becomes sharable with another subject (e.g., the creation of a child or the passing of the pipe's descriptor to another subject). At each point that the unnamed pipe is shared, the sharing must be auditable.

I-0073 OK to audit decision regardless of whether action completed

This interpretation is effective 1993-10-20 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall be able to record the following types of events: ... introduction of objects into a user's address space (e.g., file open, program initiation), ..."

> Auditing the attempted introduction of an object at the point of passing the security access control checks satisfies the above requirement, even though the object may not actually be introduced into the subject's address space because of failing later checks not related to security.

I-0084 Audit least disruptive action

This interpretation is effective 1994-07-12 and applies to classes B3 and A1.

The following interprets the requirement that "...and if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event."

> The action taken to terminate an imminent violation shall eliminate the capability to repeat the event, at least until a recurrence of the event would not indicate an imminent violation. The product developer shall provide a convincing argument for why the proposed action is the "least disruptive" of possible actions.

I-0172 Audit of imminent security violations

This interpretation is effective 1994-04-19 and applies to classes B3 and A1.

The following interprets the requirement that "The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded..."

> Audit of imminent violations is required only for actions that may lead to an actual violation (i.e., multiple failed login attempts, excessive use of identified auditable covert channels). The threshold for notification of the security administrator may be either settable by an administrator or fixed by the vendor. There shall be an immediate notification mechanism included with the product (e.g., a message to an identified terminal, a red light as part of the hardware), and the TFM shall describe how the security administrator can monitor this mechanism.

I-0286 Auditing unadvertised TCB interfaces

This interpretation is effective 1994-04-18 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall be able to record the following types of events: ... and other security-relevant events".

> The TCB shall be capable of auditing all security-relevant events that can occur during the operation of the evaluated configuration, including events that may result from the use of TCB interfaces not advertised for general use.

2.2 Configuration Management

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NO REQUIREMENT.*

B2: *NEW:* During development and maintenance of the TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *CHANGE:* During **the entire life-cycle, i.e., during the design, development,** and maintenance of the TCB, a configuration management system shall be in place **for all security-relevant hardware, firmware, and software** that maintains control of changes to **the formal model,** the descriptive **and formal** top-level **specifications**, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. Also available shall be tools, **maintained under strict configuration control,** for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

ADD: A combination of technical, physical, and procedural safeguards shall be used to protect from unauthorized modification or destruction the master copy or copies of all material used to generate the TCB.

I-0285 CM comparison source or object?

This interpretation is effective 1994-04-19 and applies to classes B2, B3, and A1.

The following interprets the B2 requirement that "Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the version of the TCB." Also interpreted is the A1 change that "Also available shall be tools, maintained under strict configuration control, ..."

> The tools and procedures used in comparing two versions of the TCB shall be able to show a mapping between the design descriptions of intended changes to the TCB and the actual changes in the compared TCB versions. The comparison tools shall operate on either or both of the TCB source code and TCB object code.

2.3 Covert Channel Analysis

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NO REQUIREMENT.*

B2: *NEW:* The system developer shall conduct a thorough search for covert storage channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.)

B3: *CHANGE:* The system developer shall conduct a thorough search for **covert channels** and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel.

A1: *ADD:* Formal methods shall be used in the analysis.

2.4 Design Documentation

C1: *NEW:* Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

C2: *NO ADDITIONAL REQUIREMENT.*

B1: *ADD:* An informal or formal description of the security policy model enforced by the TCB shall be available and an explanation provided to show that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model.

B2: *CHANGE:* **The** interfaces between **the TCB** modules shall be described. **A formal** description of the security policy model enforced by the TCB shall be available and **proven** that it is sufficient to enforce the security policy.

ADD: The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.)

B3: *ADD:* The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the DTLS. The elements of the DTLS shall be shown, using informal techniques, to correspond to the elements of the TCB.

A1: *CHANGE:* The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the **formal top-level specification (FTLS)**. The elements of the **FTLS** shall be shown, using informal techniques, to correspond to the elements of the TCB.

ADD: Hardware, firmware, and software mechanisms not dealt with in the FTLS but strictly internal to the TCB (e.g., mapping registers, direct memory access I/O) shall be clearly described.

I-0192 Interface manuals as design documentation

This interpretation is effective 1994-04-19 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirement that "Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB."

Interface-reference manuals (e.g., UNIX manual pages) are not sufficient, by themselves, as TCB design documentation.

I-0193 Standard system books as design documentation

This interpretation is effective 1993-10-20 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirement that "Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB".

> Books describing the design and implementation of a system used as the basis for a trusted system, but which are inaccurate or incomplete for the trusted system implementation, are not sufficient as design documentation. Such books may partially fulfill the requirement if additional documentation provides a complete description of all differences between the book's description and the actual system implementation, including a satisfactory description of any parts of the TCB not described in the book(s).

2.5 Design Specification and Verification

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NEW:* An informal or formal model of the security policy supported by the TCB shall be maintained over the life cycle of the ADP system that is shown to be consistent with its axioms.

B2: *CHANGE:* **A formal** model of the security policy supported by the TCB shall be maintained over the life cycle of the ADP system that is **proven** consistent with its axioms.

ADD: A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface.

B3: *ADD:* A convincing argument shall be given that the DTLS is consistent with the model.

A1: *CHANGE:* **The FTLS** shall be shown to be an accurate description of the TCB interface. A convincing argument shall be given that the DTLS is consistent with the model **and a combination of formal and informal techniques shall be used to show that the FTLS is consistent with the model**.

ADD: A formal top-level specification (FTLS) of the TCB shall be maintained that accurately describes the TCB in terms of exceptions, error messages, and effects. The DTLS and FTLS shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface. This verification evidence shall be consistent with that provided within the state-of-the-art of the particular Computer Security Center-endorsed formal specification and verification system used. Manual or other mapping of the FTLS to the TCB source code shall be performed to provide evidence of correct implementation.

I-0254 UNIX-style manual pages as DTLS

This interpretation is effective 1994-12-05 and applies to classes B2, B3, and A1.

The following interprets the requirement that "A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface."

> When complete and accurate, documentation in the style of UNIX "manual pages" is sufficient to satisfy the requirement for a DTLS.

2.6 Device Labels

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NO REQUIREMENT.*

B2: *NEW:* The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

I-0007 Assigning device level range

This interpretation is effective 1993-10-20 and applies to classes B2, B3, and A1.

The following interprets the requirement that "The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices."

> For each device, minimum and maximum security levels shall be specifiable (e.g., by request to the vendor, during system generation, during system operation) by an administrator of the system. The ability to change device security levels shall be restricted to authorized individuals.

2.7 Discretionary Access Control

C1: *NEW:* The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both.

C2: *CHANGE:* The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups **of individuals**, or by both, **and shall provide controls to limit propagation of access rights.**

ADD: The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

B1: *NO ADDITIONAL REQUIREMENT.*

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *CHANGE:* The enforcement mechanism (**e.g., access control lists**) shall allow users to specify and control sharing of those **objects,** and shall provide controls to limit propagation of access rights. These access controls shall be capable of **specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object**.

ADD: Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given.

A1: *NO ADDITIONAL REQUIREMENT.*

I-0002 Delayed revocation of DAC access

This interpretation is effective 1993-10-20 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system."

A TCB is not required to provide any mechanism for the immediate revocation of DAC access to an object where access has already been established (e.g., opened) when access to that object is reduced. It is sufficient for the SFUG and other documentation to describe the product's revocation policy. However, a change in DAC permissions shall have an immediate effect on attempts to establish new access to that object.

I-0020 DAC authority for assignment

This interpretation is effective 1993-10-20 and applies to classes C1, C2, B1, B2, B3, and A1.

Starting at C1 the following interprets the requirement that "The enforcement mechanism ... shall allow users to specify and control sharing ..." At C2 it also interprets the requirement that "Access permission ... shall only be assigned by authorized users."

> A TCB need not provide all users with the capability to control the sharing of objects. A DAC policy where only system administrators assign access to objects can satisfy the DAC requirement. The SFUG shall clearly identify the roles or user types (e.g., system administrator) who can control sharing.

I-0053 Public objects and DAC

This interpretation is effective 1995-01-12 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the entire Discretionary Access Control requirement.

> An object for which the TCB unconditionally permits all subjects "read" access shall be considered a public object, provided that only the TCB or privileged subjects may create, delete, or modify the object. No discretionary access checks or auditing are required for "read" accesses to such objects. Attempts to create, delete, or modify such objects shall be considered security-relevant events, and, therefore, controlled and auditable. Objects that all subjects can read must be, implicitly, system low.

I-0222 Passwords not acceptable for DAC

This interpretation is effective 1994-12-05 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirement that "The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both."

> The TCB shall not depend solely on passwords as an access control mechanism. If passwords are employed as part of an access control mechanism, they shall not be considered sufficient to satisfy any aspect of the DAC requirement.

I-0312 Set-ID and the DAC requirement

This interpretation is effective 1994-04-19 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the entire DAC requirement and applies to products that implement a mechanism similar to the set-user ID/set-group ID (set-ID) mechanism defined in IEEE Standard P1003.1.

The set-ID mechanism can be part of an acceptable DAC implementation.

2.8 Exportation of Labeled Information

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NEW:* The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device.

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

2.9 Exportation to Multilevel Devices

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NEW:* When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

2.10 Exportation to Single-Level Devices

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NEW:* Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

2.11 Identification and Authentication

C1: *NEW:* The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user.

C2: *ADD:* The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

B1: *CHANGE:* Furthermore, the TCB shall **maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user**.

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

I-0001 Delayed enforcement of authorization change

This interpretation is effective 1994-04-19 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirements that at C1 "The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user." and at B1 "Furthermore, the TCB shall maintain ... information for determining the clearance and authorizations of individual users. This data shall be used ... to ensure that the security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user."

> If a TCB supports security-relevant authorizations then it shall provide a method for immediate enforcement of removing those authorizations. However, the immediate method (e.g., shutting the system down) need not be the usual method for enforcement. The TFM shall describe both the usual enforcement of granting and removing authorizations and, if the immediate enforcement method is different from the usual one, how an administrator can cause immediate enforcement.

I-0096 Blanking passwords

This interpretation is effective 1994-04-18 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user."

The TCB shall not produce a visible display of any authentication data entered through the keyboard (e.g., by echoing).

I-0240 Passwords may be used for card input

This interpretation is effective 1993-10-20 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirement that "Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user."

The card input of batch jobs may contain human-readable user passwords. The TFM and the SFUG for the product shall explain the risks in placing passwords on card input and shall suggest procedures to mitigate that risk.

I-0288 Actions allowed before I&A

This interpretation is effective 1994-04-18 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate."

Prior to having been identified and authenticated by the TCB, a user communicating with the TCB may be allowed to perform only those actions that would not require TCB mediation.

2.12 Label Integrity

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NEW:* Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

2.13 Labeling Human-Readable Output

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NEW:* The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the overall sensitivity of the output or that properly[1] represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

I-0022 One set of banner pages around multiple outputs

This interpretation is effective 1994-04-19 and applies to classes B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output with human-readable sensitivity labels that properly represent the sensitivity of the output." and applies only to TCBs that allow a user to group multiple printer outputs, produced by that user, between a single set of banner pages.

> The sensitivity labels on the banner pages shall dominate the label of any individual output grouped between any single set of banner pages.

I-0039 Multilevel printers and page labeling

This interpretation is effective 1993-10-20 and applies to classes B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page."

[1] The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

For each printer included in a product's evaluated configuration that can handle multiple levels of output without administrative intervention (i.e., that is used as a multilevel device), the TCB shall be capable of marking at least one form of the printer's output (e.g., text output) with a label at the top and bottom of each page as required.

I-0040 Requirements for overwrite label capability

This interpretation is effective 1993-10-20 and applies to classes B1, B2, B3, and A1.

The following interprets the requirement that "Any override of these marking defaults shall be auditable by the TCB."

If a product allows the TCB-produced marking defaults to be overwritten, the use of this capability is equivalent to an override of marking defaults and shall be auditable.

I-0253 Default page marking format

This interpretation is effective 1994-11-16 and applies to classes B1, B2, B3, and A1.

The following interprets the requirement that "The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page."

When the TCB applies default markings on printed output, at least one line shall be reserved for the top and bottom labels and those page labels shall be clearly recognizable. Labels that are in the same font (size and type) as the adjacent user data and are not separated by white space or some other delimiter (e.g., boxes), are not sufficiently distinct. Page labels shall be positioned to ensure that alignment of the paper within customary tolerance cannot result in the loss of the labels at the top or bottom of the page. All user output on the page shall be located below the top label and above the bottom label. Each top and bottom page marking shall indicate if the human readable representation of the label does not fit in the reserved area by printing as much of the label as possible followed by some indication that the whole label was not printed (e.g., label - (more)).

I-0275 Single-level printers and page labeling

This interpretation is effective 1993-10-20 and applies to classes B1, B2, B3, and A1.

The following interprets the requirements that "The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page ..."

If a printer has been designated single-level (i.e., administrative intervention is required to change the TCB's understanding of the label of the printer and labels are not placed on the printed output by the TCB), it is acceptable to ensure that output is properly marked on the banner pages and at the top and bottom of each page by administratively controlled, procedural means (e.g., use pre-marked paper, stamp each page after the output is removed from the printer). The TFM shall describe how the product can facilitate the procedural enforcement of labeling output from single-level printers.

2.14 Labels

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NEW:* Sensitivity labels associated with each subject and storage object under its control (e.g., process, file, segment, device) shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

B2: *CHANGE:* Sensitivity labels associated with each **ADP system resource (e.g., subject, storage object, ROM) that is directly or indirectly accessible by subjects external to the TCB** shall be maintained by the TCB.

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

2.15 Mandatory Access Control

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NEW:* The TCB shall enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices). These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between subjects and objects controlled by the TCB: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level. Identification and authentication data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorization of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user.

B2: *CHANGE:* The TCB shall enforce a mandatory access control policy over all **resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB**. The following requirements shall hold for all accesses between **all subjects external to the TCB and all objects directly or indirectly accessible by these subjects**.

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

I-0003 Access validation after object label change

This interpretation is effective 1994-11-16 and applies to classes B1, B2, B3, and A1.

The following interprets the entire MAC requirement and applies only if the TCB provides an interface for changing an object's label.

> The MAC policy shall be enforced with respect to the new label for all data written to the object after the label change is completed successfully. The label change shall be considered complete when an access control check would be made with respect to the new value of the label; this shall occur no later than when an indication of completion is returned by the TCB to the agent (e.g., user, process) requesting the change. The TFM, and SFUG, if appropriate, shall describe the effects of label changes on access to objects. It is not acceptable for access changes resulting from object label changes to be enforced only through procedural means.

I-0239 Subject access revocation after change in user clearance

This interpretation is effective 1994-04-19 and applies to classes B1, B2, B3, and A1.

The following interprets all of the MAC requirement.

> If a system allows an administrator to change the MAC subject security database values (e.g., the clearance range for a user), the TFM shall describe how the change can be accomplished while still enforcing the system's MAC policy as specified in the security database. A procedure followed by an administrator is sufficient for the enforcement of the policy if it is easy to ensure that the values in the database control all subsequent actions (e.g., read from a file, no batch jobs run under the wrong clearance). If the procedure is too complicated, TCB enforcement shall be required.

2.16 Object Reuse

C1: *NO REQUIREMENT.*

C2: *NEW:* All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

B1: *NO ADDITIONAL REQUIREMENT.*

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

I-0041 Object reuse applies to all system resources

This interpretation is effective 1994-04-19 and applies to classes C2, B1, B2, B3, and A1.

The following interprets all of the Object Reuse requirement.

> Analysis for residual data shall be performed on all sharable objects and their attributes (i.e., objects to which MAC or DAC are applied) and other system resources (e.g., stacks, process memory).

2.17 Security Features User's Guide

C1: *NEW:* A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

C2: *NO ADDITIONAL REQUIREMENT.*

B1: *NO ADDITIONAL REQUIREMENT.*

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

I-0244 Flexibility in packaging SFUG

This interpretation is effective 1993-10-20 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the entire SFUG requirement.

> All SFUG documentation shall be in a form that system administrators and users can read at the time that an understanding of the topics covered is needed to use the system in a secure manner (e.g, it shall not be required that the user login in order to read instructions about how to login). The documents or portions of documents that make up the SFUG shall be precisely identified. There are no further restrictions on the packaging (one document, several documents, parts of several documents) or delivery (hardcopy, online) of the SFUG.

2.18 Security Testing

C1: *NEW:* The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. (See the Security Testing guidelines.)

C2: *ADD:* Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

B1: *NEW:* The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. All discovered flaws shall be removed or neutralized and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. (See the Security Testing Guidelines.)

B2: *CHANGE:* All discovered flaws shall be **corrected** and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced.

ADD: The TCB shall be found relatively resistant to penetration. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification.

B3: *CHANGE:* The TCB shall be **found resistant to** penetration.

ADD: No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain.

A1: *CHANGE:* Testing shall demonstrate that the TCB implementation is consistent with the **formal** top-level specification.

ADD: Manual or other mapping of the FTLS to the source code may form a basis for penetration testing.

I-0170 Functional tests required for object reuse

This interpretation is effective 1994-04-18 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirement that "The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB."

> TCB interface(s) that allow manipulation and review of the contents of a subject's address space and of other resources available at the TCB interface (storage and named objects, devices) shall have functional tests included in the vendor test suite to supplement the analysis for object reuse.

2.19 Subject Sensitivity Labels

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NO REQUIREMENT.*

B2: *NEW:* The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

2.20 System Architecture

C1: *NEW:* The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

C2: *ADD:* The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

B1: *ADD:* The TCB shall maintain process isolation through the provision of distinct address spaces under its control.

B2: *NEW:* The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified.

B3: *ADD:* The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system. The TCB shall incorporate significant use of layering, abstraction and data hiding. Significant system engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are not protection-critical.

A1: *NO ADDITIONAL REQUIREMENT.*

I-0213 Administrator interface is part of TCB

This interpretation is effective 1995-01-12 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirement at C2 that "The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements."

> Those components of the product that provide the interfaces required for performing administrative actions shall be considered TCB components.
>
> The "administrative actions" to which this interpretation applies shall be those that are defined in the TFM to be performed by administrative personnel (e.g., operators, system administrators, system security officers) while the product is in its secure operational state. The TFM shall clearly identify which mechanisms are, and which are not, acceptable for performing each administrative action.

2.21 System Integrity

C1: *NEW:* Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

C2: *NO ADDITIONAL REQUIREMENT.*

B1: *NO ADDITIONAL REQUIREMENT.*

B2: *NO ADDITIONAL REQUIREMENT.*

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *NO ADDITIONAL REQUIREMENT.*

I-0144 Availability of diagnostics

This interpretation is effective 1994-11-16 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the entire System Integrity requirement.

> If the features provided by the vendor to meet this requirement cannot be exercised by the purchaser of the product, the vendor shall make available appropriate services to use the features as needed to meet the requirement. These services shall be available on an "on-demand" basis.

2.22 Test Documentation

C1: *NEW:* The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested and results of the security mechanisms' functional testing.

C2: *NO ADDITIONAL REQUIREMENT.*

B1: *NO ADDITIONAL REQUIREMENT.*

B2: *ADD:* It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths.

B3: *NO ADDITIONAL REQUIREMENT.*

A1: *ADD:* The results of the mapping between the formal top-level specification and the TCB source code shall be given.

2.23 Trusted Distribution

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NO REQUIREMENT.*

B2: *NO REQUIREMENT.*

B3: *NO REQUIREMENT.*

A1: *NEW:* A trusted ADP system control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version. Procedures (e.g., site security acceptance testing) shall exist for assuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies.

2.24 Trusted Facility Management

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NO REQUIREMENT.*

B2: *NEW:* The TCB shall support separate operator and administrator functions.

B3: *ADD:* The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.

A1: *NO ADDITIONAL REQUIREMENT.*

I-0315 Restricted to trusted administrative interface

This interpretation is effective 1995-01-12 and applies to classes B3 and A1.

The following interprets the requirement that "The TCB shall support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. . . . Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively."

> The interfaces specified in the TFM for performing operator, administrator, and security administrator functions shall be the only interfaces available for performing those functions while the product is in its secure operational state.

2.25 Trusted Facility Manual

C1: *NEW:* A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

C2: *ADD:* The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

B1: *ADD:* The manual shall describe the operator and administrator functions related to security, to include changing the characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner.

B2: *ADD:* The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described.

B3: *ADD:* It shall include the procedures to ensure that the system is initially started in a secure manner. Procedures shall also be included to resume secure system operation after any lapse in system operation.

A1: *NO ADDITIONAL REQUIREMENT.*

I-0046 Detailed audit record structure

This interpretation is effective 1994-07-12 and applies to classes C2, B1, B2, B3, and A1.

The following interprets the requirement that "The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given."

> The documentation of the detailed audit record structure may describe either the raw records produced by the audit mechanism or the output of an audit post-processing tool as long as the records described contain the information specified in the audit requirement. If the output of the audit post-processing tool is described, the tool is considered part of the TCB.

I-0069 Flexibility in packaging TFM

This interpretation is effective 1993-10-20 and applies to classes C1, C2, B1, B2, B3, and A1.

The following interprets the requirement that "A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility."

> All TFM documentation shall be in a form that system administrators and users can read at the time that an understanding of the topics covered is needed to use the system in a secure manner (e.g., it shall not be required that the system be brought up in order to read instructions about

how to bring up the system). The documents or portions of documents that make up the TFM shall be precisely identified. There are no further restrictions on the packaging (one document, several documents, parts of several documents) or delivery (hardcopy, online) of the TFM.

2.26 Trusted Path

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NO REQUIREMENT.*

B2: *NEW:* The TCB shall support a trusted communication path between itself and user for initial login and authentication. Communications via this path shall be initiated exclusively by a user.

B3: *CHANGE:* The TCB shall support a trusted communication path between itself and **users** for **use when a positive TCB-to-user connection is required (e.g., login, change subject security level)**. Communications via this **trusted** path shall be **activated** exclusively by a user **or the TCB and shall be logically isolated and unmistakably distinguishable from other paths**.

A1: *NO ADDITIONAL REQUIREMENT.*

2.27 Trusted Recovery

C1: *NO REQUIREMENT.*

C2: *NO REQUIREMENT.*

B1: *NO REQUIREMENT.*

B2: *NO REQUIREMENT.*

B3: *NEW:* Procedures and/or mechanisms shall be provided to assure that, after an ADP system failure or other discontinuity, recovery without a protection compromise is obtained.

A1: *NO ADDITIONAL REQUIREMENT.*

Chapter 3

Interpretation Rationale

This chapter lists the set of interpretations along with any applicable evaluation impacts and their supporting rationale. They are ordered by their unique interpretation numbers and are identified by that number and a name. For each interpretation, there is an indication of the effective date, applicable criteria, and applicable levels of trust. There is also an indication of the user documentation (i.e., the SFUG or TFM) that may be affected by the interpretation, if appropriate. Subsequently, there is an indication of any related interpretations and the interpretation statement itself. Each interpretation is followed by any applicable evaluation impacts and then by supporting rationale. Note that the evaluation impact was relevant at the time the interpretation was approved; if there is no stated impact it was considered negligible. The support is essentially the rationale behind the interpretations.

I-0001 Delayed enforcement of authorization change

This interpretation is effective 1994-04-19 and applies to **Identification and Authentication**, *classes C1, C2, B1, B2, B3, and A1.*

This interpretation affects the TFM.

See related interpretations "**I-0002** Delayed revocation of DAC access", "**I-0003** Access validation after object label change", "**I-0004** Enforcement of audit settings consistent with protection goals", and "**I-0239** Subject access revocation after change in user clearance".

The following interprets the requirements that at C1 "The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user." and at B1 "Furthermore, the TCB shall maintain ... information for determining the clearance and authorizations of individual users. This data shall be used ... to ensure that the security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user."

> If a TCB supports security-relevant authorizations then it shall provide a method for immediate enforcement of removing those authorizations. However, the immediate method (e.g., shutting the system down) need not be the usual method for enforcement. The TFM shall describe both the usual enforcement of granting and removing authorizations and, if the immediate enforcement method is different from the usual one, how an administrator can cause immediate enforcement.

Support

The term "security-relevant authorization" is used here to mean a capability, assigned administratively to some user or users, to perform security-relevant operations not permitted ordinary, untrusted users (e.g.,

in Secureware type Unix systems, privileges). The term "authorization" is not intended to cover controls on routine access to data by untrusted users; that is handled through the DAC and MAC mechanisms. Examples of authorizations include:

- Ability to act as system administrator
- Ability to set audit control parameters
- Ability to act as system operator
- Ability to manipulate others' requests in printer queues
- Ability to use unlabeled import/export media
- Ability to change other user's passwords
- Ability to downgrade objects

Many authorizations could have serious consequences if misused, so an immediate revocation method must exist. In most situations (e.g., a change in job responsibilities), immediate enforcement is not required.

I-0002 Delayed revocation of DAC access

This interpretation is effective 1993-10-20 and applies to **Discretionary Access Control**, *classes C1, C2, B1, B2, B3, and A1.*

This interpretation affects the SFUG.

See related interpretations "**I-0001** Delayed enforcement of authorization change", "**I-0003** Access validation after object label change", "**I-0004** Enforcement of audit settings consistent with protection goals", and "**I-0239** Subject access revocation after change in user clearance".

The following interprets the requirement that "The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system."

> A TCB is not required to provide any mechanism for the immediate revocation of DAC access to an object where access has already been established (e.g., opened) when access to that object is reduced. It is sufficient for the SFUG and other documentation to describe the product's revocation policy. However, a change in DAC permissions shall have an immediate effect on attempts to establish new access to that object.

Support

DAC policies may vary and can include immediate revocation (e.g., Multics immediately revokes access to segments) or delayed revocation (e.g., most UNIX systems do not revoke access to already opened files). DAC permission is considered to have been revoked when all subsequent access control decisions by the TCB

use the new access control information. It is not required that every operation on an object make an explicit access control decision as long as a previous access control decision was made to permit that operation.

The TCSEC does not specify a restrictive definition of legal DAC policies and, therefore, wide variances are permissible. It is sufficient that the vendor clearly document how revocation is enforced, and consumers must choose the product that best fits their needs.

I-0003 Access validation after object label change

This interpretation is effective 1994-11-16 and applies to **Mandatory Access Control**, *classes B1, B2, B3, and A1.*

This interpretation affects both the SFUG and TFM.

See related interpretations "**I-0001** Delayed enforcement of authorization change", "**I-0002** Delayed revocation of DAC access", "**I-0004** Enforcement of audit settings consistent with protection goals", and "**I-0239** Subject access revocation after change in user clearance".

The following interprets the entire MAC requirement and applies only if the TCB provides an interface for changing an object's label.

> The MAC policy shall be enforced with respect to the new label for all data written to the object after the label change is completed successfully. The label change shall be considered complete when an access control check would be made with respect to the new value of the label; this shall occur no later than when an indication of completion is returned by the TCB to the agent (e.g., user, process) requesting the change. The TFM, and SFUG, if appropriate, shall describe the effects of label changes on access to objects. It is not acceptable for access changes resulting from object label changes to be enforced only through procedural means.

Impact

Most evaluated products meet this interpretation.

Support

Products that permit object labels to be changed, by methods specified in the TFM, are still required to enforce at all times their MAC policy on defined storage objects; however, a number of mechanisms or restrictions would be satisfactory methods of enforcement. For example, the TCB could satisfy this requirement by preventing changes to an object's label while any subject has active access (e.g., possesses a descriptor for the object), or preventing the label change only if it would result in an active subject acquiring access not permitted by the MAC policy. Another acceptable, and more versatile and secure, enforcement mechanism would be to recalculate each subject's access when the label is changed, or, less flexibly, simply to revoke access for all subjects. The point is that the MAC policy must be continuously enforced: object label changes must not permit access that violates the policy.

> "Procedural" in this context means that the TFM describes a step-by-step process for changing an object label. If the procedure is not followed correctly illegal information flows could occur.

A naive view of revocation would be that a subsequent "read" or "fetch" from the object must fail if the subject's label does not dominate the object's new label. In practice, buffering makes this analysis complex, because data may have been copied (by the TCB) between the object's "permanent" storage representation and buffers from which the "read" operation actually retrieves data. For instance, if an operating system implements read-ahead for files, or reads a block at a time, a sequence of user-visible "read" operations requesting one byte at a time may succeed even though the real object's label has changed. Similarly, in a DBMS, a "select" operation may identify a set of tuples and create a logical copy of the set from which individual tuples can be fetched.

In all cases, however, the critical issue is that subsequent information flows must be prevented after the label change. If the following sequence of operations occurs:

Object contains "A" Subject1 opens object File label changes so that subject1 can no longer read it Subject2 writes "B" to file

a subsequent "read" by subject1 may result in an error, or may validly return "A", because those were the contents before the label change, but it MUST NOT return "B", because that would make visible a change of contents that occurred after the label change.

In most products, such buffering and concurrency control issues have little practical effect, because it is important to maintain consistency between different subjects' views of an object–if not immediately, then usually within a granularity of a few seconds or a few thousand bytes. In products such as DBMSs, however, where subjects exercise explicit control over consistency and concurrency, the window of inconsistent access may be significantly larger, because consistency is of greater concern to applications. The size of the window is not an issue, as long no invalid flows occur after the label change is committed. The documentation (TFM, SFUG) should describe the effects of access changes so that administrators and users can understand the risks of changing labels.

Because some object label changes may be under the control of untrusted users, it is critically important to the MAC policy that the TCB enforce that the change be effective. Automatic enforcement of the label change is necessary because it would be infeasible to rely on procedures for protection against active attack (manipulation) of the objects by untrusted subjects. For example, in a system where an untrusted user is permitted to upgrade an object, it would be unreasonable to depend on that user to block all access to the object, then check for other subjects with current access to it, before making the label change. Yet, if that procedure were not followed, an existing subject might retain access to the object, and thus be able to violate the system's MAC policy.

In many instances, trusted users who are given the privilege to downgrade are not system administrators, but are either system security officers or security officers for a particular application domain. They may have little understanding of the product and therefore have difficulty following a procedure or recovering from mistakes. Without the aid of the TCB even system administrators would find it very difficult on most systems to change the level of an object on an actively running system and ensure that no window of opportunity for illegal access exists without the aid of the TCB; therefore, procedural means are not sufficient.

The TCB may provide multiple means for trusted users to change object labels, some of which do not enforce the MAC policy. This may be acceptable, subject to other requirements (e.g., system architecture, trusted facility management), as long as the TFM advises use of the MAC policy enforcing mechanisms and explains

the risk of using the non-MAC policy enforcing mechanisms.

I-0004 Enforcement of audit settings consistent with protection goals

This interpretation is effective 1993-10-20 and applies to **Audit**, *classes C2, B1, B2, B3, and A1.*

This interpretation affects the TFM.

See related interpretations "**I-0001** Delayed enforcement of authorization change", "**I-0002** Delayed revocation of DAC access", "**I-0003** Access validation after object label change", and "**I-0239** Subject access revocation after change in user clearance".

The following interprets the requirement that "The ADP system administrator shall be able to selectively audit . . ."

> If the TCB supports the selection of events to be audited, it shall provide a method for immediate enforcement of a change in audit settings (e.g., to audit a specified user, to audit objects at a particular sensitivity level); however, the immediate method (e.g., shutting the system down) need not be the usual method for enforcement. The TFM shall describe both the usual enforcement of audit settings and, if the immediate enforcement method is different from the usual one, how an administrator can cause immediate enforcement.
>
> The TFM shall describe the consequences of changing an audit state dynamically if such changes could result in incomplete or misleading audit data.

Support

It is preferable to have the TCB audit mechanism ensure that enforcement occurs in a timely manner, consistent with the system's design and protection goals. However, "timely" is a subjective term and the TCSEC does not include such a requirement, although the control objectives say that audit data should be collectable within a reasonable time and without undue difficulty. Therefore, it is sufficient that the vendor clearly document how audit setting changes are enforced, and consumers must choose the product that best fits their needs.

Sometimes, if the quantity or detail of auditing is increased, it may not be possible for the system to generate informative audit records about existing subjects. For instance, if a system identifies users in audit records on the basis of a numeric process ID and a mapping from user name to process ID is normally created at user login, if audit for a user is turned on after login, that user's audit records will not be meaningful. The TFM guidance for this situation would need to describe the consequence of not collecting audit records from the time of login (and would likely need to recommend that login audit records always be collected, regardless of what other events are audited).

I-0005 Action for audit log overflow

This interpretation is effective 1993-10-20 and applies to **Audit**, *classes C2, B1, B2, B3, and A1.*

This interpretation affects the TFM.

The following interprets the requirement that "The TCB shall be able to create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects."

> When the TCB becomes unable to collect audit data, it shall give a clear indication of this condition and take a pre-specified action. The system implementation may allow an administrator to choose from a range of actions. One of the actions that may be chosen by the administrator (or, if no choice is possible, the only action) shall be that the system cease performing auditable events when the TCB is unable to collect audit data. Choosing an audit overflow action shall be considered a security-relevant administrative event for the purposes of auditing. The TFM shall fully describe the administrator's options.

Support

This is a restatement of formal interpretation C1-CI-01-89, modified slightly to eliminate its unsupportable requirement for a "default" action. The system may be delivered without the most restrictive action pre-set, as long as the TFM clearly explains the options and how to configure the system not to lose audit data as a result of audit log overflow.

In order to maintain an accurate audit trail, the administrator must have the capability to stop auditable actions whenever it is impossible to audit them (e.g., halt temporarily, shut down). To allow flexibility when performance is more important than the loss of audit data, a system may provide other possible options when auditing is impossible (e.g., discard some or all audit data, overwrite existing audit data, request new audit media).

This interpretation requires that appropriate action be taken any time the TCB detects that audit data are being lost or are otherwise not collectable, whether because of, for example, overflow of permanent storage or lack of space in internal buffers. This interpretation is limited to losses that are detected during collection; the loss of already collected and permanently stored audit data is not covered here.

The intent of this interpretation is to encourage vendors to provide a choice of action, since different operational environments clearly have different needs: one administrator may prefer to continue operating and overwrite old audit data, when operation is more important than accountability, whereas another administrator might consider accountability more important and want to retain the audit trail even at the expense of losing function. However, if no choice is permitted, the only action that can meet the TCSEC requirement to "maintain and protect" the audit trail is to cease performing auditable events altogether when the audit trail is unavailable.

I-0006 Audit of user-id for invalid login

This interpretation is effective 1993-10-20 and applies to **Audit**, *classes C2, B1, B2, B3, and A1.*

This interpretation affects the TFM.

The following interprets the requirement that "The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, ... For each recorded event, the audit record

shall identify: date and time of the event, user, type of event, and success or failure of the event."

> While the audit mechanism is required to be capable of producing a record of each login attempt, on failed login attempts it is not required to record in the audit record the character string supplied as the user identity.

Support

This is a restatement of formal interpretation C1-CI-01-84.

Recording the character string on failed login attempts would have the positive aspect of possibly allowing the auditor to identify some types of break-in attempts. It would have the negative aspect of exposing the user's password in the audit log whenever a user mistakenly types a password when an identifier is requested. A flexible implementation would allow the system administrator to decide whether the increased ability to detect break-in attempts is worth the risk of possible password exposure.

I-0007 Assigning device level range

This interpretation is effective 1993-10-20 and applies to **Device Labels**, *classes B2, B3, and A1.*

This interpretation affects the TFM.

The following interprets the requirement that "The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices."

> For each device, minimum and maximum security levels shall be specifiable (e.g., by request to the vendor, during system generation, during system operation) by an administrator of the system. The ability to change device security levels shall be restricted to authorized individuals.

Support

This is a restatement of formal interpretation C1-CI-01-85.

The requirement for maximum and minimum security levels would be vacuous if those levels were not settable.

This interpretation is specifically intended to allow device label ranges to be preconfigured by the vendor (to customer specifications) before the product is even delivered. This may be appropriate, for example, in a network routing product where the label configuration is burned into PROM and there is no requirement for dynamic changes.

I-0020 DAC authority for assignment

This interpretation is effective 1993-10-20 and applies to **Discretionary Access Control**, *classes C1, C2, B1, B2, B3, and A1.*

Starting at C1 the following interprets the requirement that "The enforcement mechanism ... shall allow users to specify and control sharing ..." At C2 it also interprets the requirement that "Access permission ... shall only be assigned by authorized users."

> A TCB need not provide all users with the capability to control the sharing of objects. A DAC policy where only system administrators assign access to objects can satisfy the DAC requirement. The SFUG shall clearly identify the roles or user types (e.g., system administrator) who can control sharing.

Support

This restates formal interpretation C1-CI-03-85 and extends it to C1.

Products vary regarding their definition of "authorized users" and "assign". UNIX systems usually make the creator of an object the "owner", the only untrusted user who can alter the access control data. Multics included the ability to specify in the access control data who can modify such data. A few products, mostly those with access profiles attached to the user rather than access lists attached to the object, allow only users in the system administrator role to alter the access control data. All of these variations are legal DAC policies. The administrator-controlled policy has to ensure that, if untrusted subjects are allowed to create objects, no untrusted subject has access to newly created objects until the necessary administrative action is performed.

I-0022 One set of banner pages around multiple outputs

This interpretation is effective 1994-04-19 and applies to **Labeling Human Readable Output**, *classes B1, B2, B3, and A1.*

The following interprets the requirement that "The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output with human-readable sensitivity labels that properly represent the sensitivity of the output." and applies only to TCBs that allow a user to group multiple printer outputs, produced by that user, between a single set of banner pages.

> The sensitivity labels on the banner pages shall dominate the label of any individual output grouped between any single set of banner pages.

Support

Grouping multiple outputs belonging to a single user between proper banner pages with suitable page labels does not lessen a site's ability to handle sensitive printer output securely, except that some or all of the individual outputs may be overclassified by the markings on the banner pages. Products that automatically label banner pages with the subject's sensitivity label sometimes overclassify output, although they certainly meet the labeling requirements. If the product can ensure that the label on the printed output properly represents the sensitivity of the data in the object being printed, then the banner page labels may be lower than the subject's label.

An information flow can result from labeling output lower than the subject's label. The flow can be to a person watching printer output or to any subject who is restricted only by MAC access to the list of objects on the printer queue. Such an information flow could be permissible at B1 and subject to covert channel analysis at B2 and above.

Various ways exist to determine the best banner page sensitivity label to place on grouped outputs. For example, it could be the greatest sensitivity label of the individual outputs, if that label dominates all of the other labels in the grouping. The TCB could also compute the least upper bound of the individual labels, if that label is valid on the system. Some products may support the concept of undefined points on the security label lattice. These products could compute a least upper bound on a group of outputs that is not valid (i.e., is undefined). Other products assume that all points on the lattice are defined (valid), even if no human-readable name has been assigned to them.

In general, output from different users should not be grouped under a single set of banner pages.

I-0039 Multilevel printers and page labeling

This interpretation is effective 1993-10-20 and applies to **Labeling Human Readable Output**, *classes B1, B2, B3, and A1.*

See related interpretations "**I-0040** Requirements for overwrite label capability" and "**I-0253** Default page marking format".

The following interprets the requirement that "The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page."

> For each printer included in a product's evaluated configuration that can handle multiple levels of output without administrative intervention (i.e., that is used as a multilevel device), the TCB shall be capable of marking at least one form of the printer's output (e.g., text output) with a label at the top and bottom of each page as required.

Impact

This reverses previous guidance that said as long as one available printer supports page labeling, others need not.

Support

If an evaluated configuration of the product can include printers that are used as multilevel devices and are incapable of printing page labels, it is hard to see how such a configuration can be said to print page labels "by default".

The phrase "at least one form of output" permits the inclusion of printers that cannot reliably provide page

labels on some forms of output (e.g., graphics, PostScript) as long as they possess the minimal capability of producing some useful form of output (such as ASCII text) with TCB-provided page labels.

The FER should include or reference guidance on the risk of using printers not in the evaluated configuration, or using evaluated printers with the forms of output that the TCB cannot guarantee default markings (which should cause an audit message).

I-0040 Requirements for overwrite label capability

This interpretation is effective 1993-10-20 and applies to **Labeling Human Readable Output**, *classes B1, B2, B3, and A1.*

See related interpretations "**I-0039** Multilevel printers and page labeling" and "**I-0253** Default page marking format".

The following interprets the requirement that "Any override of these marking defaults shall be auditable by the TCB."

> If a product allows the TCB-produced marking defaults to be overwritten, the use of this capability is equivalent to an override of marking defaults and shall be auditable.

Support

A trusted product must be capable of labeling the top and bottom of pages of output. If a subject requests that the TCB turn off default markings, that is an "override". If a subject has access to the complete output page and can place data in the areas normally reserved for default markings without asking the TCB, that is an "overwrite". If a product has the capability to overwrite default markings, the TCB must be able to detect when the capability to overwrite default markings can be used and audit such use.

I-0041 Object reuse applies to all system resources

This interpretation is effective 1994-04-19 and applies to **Object Reuse**, *classes C2, B1, B2, B3, and A1.*

The following interprets all of the Object Reuse requirement.

> Analysis for residual data shall be performed on all sharable objects and their attributes (i.e., objects to which MAC or DAC are applied) and other system resources (e.g., stacks, process memory).

Support

Shared objects and the subject's address space are possible vehicles for carrying residual data from one subject to another subject. Global pools of resources, where by individual resources are serially allocated to

one subject and then returned to the global pool, require careful examination. For shared objects, all of the object's attributes must also be examined, because their access control and method of eliminating residual data may be different than those for the object itself.

Three types of residual data exist: subject-created data with no TCB understood semantics (e.g., file contents), subject-created data with TCB understood semantics (e.g., filenames in a directory), and TCB-created data whose value the subject can influence (e.g. the modification-time attribute of a file). Not eliminating residual data in the first type can result in a direct transfer of information from one subject to another, with no intention on the part of the sending subject (or even the receiving subject). The second and third type can result in a direct transfer of information (e.g. names of files could be useful information); however, they are probably more useful for encoding information (i.e., used as a covert channel), which would usually require intention on the part of the sender and receiver.

The second and third type of residual data are often overlooked in an object reuse analysis. For example, devices have attributes that are readable, and sometimes writable, by a subject while allocated. Some of these attributes may not be reset to a standard configuration value in all situations when the device is returned to the global pool. Since these attributes have TCB-understood semantics and will not contain random residual user data, they are an example of either the second or third type.

The analysis for residual data must use the abstractions supported at the TCB interface. For example, one of the visible abstractions of many products is files, although the implementation internal to the TCB may involve segments or buffer caches.

TCB internal data structures have, at times, been considered as a factor contributing to residual data. Some products have had residual data problems because, even though they cleared shared objects and the subject's address space at creation, the TCB, as part of its execution of a subject, moved data left over from a previous subject in a TCB internal data structure to a shared object or another subject's address space. Such actions are not examples of an object reuse problem; however, they are an example of a lack of process separation or TCB isolation.

I-0043 Auditing use of unnamed pipe

This interpretation is effective 1994-04-19 and applies to **Audit***, classes C2, B1, B2, B3, and A1.*

The following interprets the requirements that "The TCB shall be able to record the following types of events: ... introduction of objects into a user's address space (e.g., file open, program initiation), ... For events that introduce an object into a user's address space..."

> In products that support mechanisms similar to unnamed pipes in UNIX systems, the creation of an unnamed pipe shall be auditable; however, the auditing may be delayed until the pipe becomes sharable with another subject (e.g., the creation of a child or the passing of the pipe's descriptor to another subject). At each point that the unnamed pipe is shared, the sharing must be auditable.

Impact

This interpretation may affect a few products; however, the majority have the audit capability.

Support

The TCSEC requires the introduction of an object into a subject's address space to be audited, and in UNIX the main purpose of unnamed pipes is to share data between parent and child or between siblings, all of whom are different subjects. When an unnamed pipe is created, it is not able to be referenced by any other subject and, therefore, need not be audited at that point. However, when a child is created with that pipe open, it is now shared and must be auditable. The auditing must indicate the introduction of the unnamed pipe into all involved subjects' address spaces (i.e., both the original holder of the object and the receiver). Since in UNIX, opened descriptors are automatically passed on to "forked" children, the audit of the unnamed pipe, either at creation or at the forking of the first child after creation, allows the audit mechanism to assume that all subsequent children have access to the unnamed pipe, except those created after pipe closure. Either the TFM should make this assumption clear to the auditor or audit log postprocessing could add to the audit information the introduction of the unnamed pipe to each child's address space.

In those products that allow descriptors to be passed across sockets, each passage of an unnamed pipe descriptor through a socket to a different subject's address space would have to be auditable.

I-0046 Detailed audit record structure

This interpretation is effective 1994-07-12 and applies to **Trusted Facility Manual**, *classes C2, B1, B2, B3, and A1.*

This interpretation affects the TFM.

The following interprets the requirement that "The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given."

> The documentation of the detailed audit record structure may describe either the raw records produced by the audit mechanism or the output of an audit post-processing tool as long as the records described contain the information specified in the audit requirement. If the output of the audit post-processing tool is described, the tool is considered part of the TCB.

Support

One purpose of the detailed audit record structure is to allow an evaluator to decide whether the records contain sufficient information to meet the audit requirement. The other purpose is to allow an administrator to implement additional post-processing of the audit data that is relevant to a particular environment. A post-processing tool supplied with the product that, for example, combines partial records to make a complete story or adds user names to records with only user ids does not prevent additional processing. But a post-processing tool that only produces summaries loses information and would not meet the audit requirement.

If the description of the detailed audit record depends upon a post-processing tool, then that tool must be treated the same as the rest of the TCB. It must be configuration managed either under RAMP or configuration management requirements, must be tested, and must meet the system architecture requirement.

I-0053 Public objects and DAC

This interpretation is effective 1995-01-12 and applies to **Discretionary Access Control**, *classes C1, C2, B1, B2, B3, and A1.*

The following interprets the entire Discretionary Access Control requirement.

> An object for which the TCB unconditionally permits all subjects "read" access shall be considered a public object, provided that only the TCB or privileged subjects may create, delete, or modify the object. No discretionary access checks or auditing are required for "read" accesses to such objects. Attempts to create, delete, or modify such objects shall be considered security-relevant events, and, therefore, controlled and auditable. Objects that all subjects can read must be, implicitly, system low.

Support

This is a restatement of formal interpretation C1-CI-03-89.

A few products have special objects that are intended for unrestricted read (or execute) access by all subjects (e.g., a public library, message of the day, time of day clock). These objects are either updated by the TCB as part of its execution or updated by system administrative actions. To qualify they also must be a separate type of object, not just a few files in the file system. Requiring the usual type of DAC mechanism on such objects is not necessary and would not increase security.

I-0069 Flexibility in packaging TFM

This interpretation is effective 1993-10-20 and applies to **Trusted Facility Manual**, *classes C1, C2, B1, B2, B3, and A1.*

This interpretation affects the TFM.

See related interpretation "**I-0244** Flexibility in packaging SFUG".

The following interprets the requirement that "A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility."

> All TFM documentation shall be in a form that system administrators and users can read at the time that an understanding of the topics covered is needed to use the system in a secure manner (e.g., it shall not be required that the system be brought up in order to read instructions about how to bring up the system). The documents or portions of documents that make up the TFM shall be precisely identified. There are no further restrictions on the packaging (one document, several documents, parts of several documents) or delivery (hardcopy, online) of the TFM.

Support

Although the literal words of the TFM requirement refer to a manual, this is not intended to restrict unduly the vendor's options in packaging the information, as long as it is clearly and concisely identified. The TFM and SFUG may be packaged in the same document, if the appropriate chapters are identified for each requirement (although in most systems untrusted users do not need access to the TFM). Some systems (e.g., certain network components) have no interface for untrusted users and therefore no SFUG. All of the TFM can be online, except for information needed before an online status can be achieved.

Although this interpretation does not restrict the packaging of the TFM, we do expect a coherent document, or documents, either in the form of one or two documents or in the form of a "road map" that clearly points to the sections of the TFM in several documents.

In all cases, it is expected that the SFUG be logically part of the TFM; that is, the administrator must be familiar with both documents in order to perform administrative duties correctly. There is no reason to duplicate SFUG contents in the TFM.

I-0073 OK to audit decision regardless of whether action completed

This interpretation is effective 1993-10-20 and applies to **Audit**, *classes C2, B1, B2, B3, and A1.*

The following interprets the requirement that "The TCB shall be able to record the following types of events: ... introduction of objects into a user's address space (e.g., file open, program initiation), ..."

> Auditing the attempted introduction of an object at the point of passing the security access control checks satisfies the above requirement, even though the object may not actually be introduced into the subject's address space because of failing later checks not related to security.

Support

A product may be designed so that an audit record is cut immediately after the access control permissions are checked. Other checks, such as those necessary for requests for exclusive use, may occur after the security checks and cause the open to fail; however, the audit record would still be in the audit log.

Although this method may create a misleading audit trail, it does provide information about what a subject attempted to access and whether the request was successful relevant to security. Even an audit of a successful open of an object does not indicate whether the subject accessed any part of the information in an object.

Note: This interpretation applies only to the introduction of an object into the subject's address space. This does not imply that incomplete auditing is either acceptable or unacceptable for other types of events.

I-0084 Audit least disruptive action

This interpretation is effective 1994-07-12 and applies to **Audit**, *classes B3 and A1.*

This interpretation affects the TFM.

The following interprets the requirement that "...and if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event."

> The action taken to terminate an imminent violation shall eliminate the capability to repeat the event, at least until a recurrence of the event would not indicate an imminent violation. The product developer shall provide a convincing argument for why the proposed action is the "least disruptive" of possible actions.

Support

"Least disruptive" applies to the other subjects, not the violators. The definition of least disruptive is often product and even environment dependent. The developer's knowledge of the market for the product and the product's design should provide a strong basis for an argument for a least disruptive action.

As examples of standard low disruption actions, for multiple login attempts the user's account or, in some cases, the terminal could be locked; for excessive use of identified auditable covert channels, access to the shared resource could be denied or the subject could be killed and the account locked.

I-0096 Blanking passwords

This interpretation is effective 1994-04-18 and applies to **Identification and Authentication**, *classes C1, C2, B1, B2, B3, and A1.*

The following interprets the requirement that "The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user."

> The TCB shall not produce a visible display of any authentication data entered through the keyboard (e.g., by echoing).

Support

While a user password change may include an authentication operation (e.g., the entry of the current password), the new password is not considered authentication data until it has been successfully changed. Therefore, a TCB generated password may be visibly displayed, but the change must not be completed until there is explicit confirmation from the user. The user must take any appropriate steps to protect the new authentication data (e.g., ensure that no one else can see the display).

In the case of hardcopy devices, the obliteration of the space where the authentication data will be placed is sufficient.

I-0144 Availability of diagnostics

This interpretation is effective 1994-11-16 and applies to **System Integrity**, *classes C1, C2, B1, B2, B3, and A1.*

This interpretation affects the TFM.

The following interprets the entire System Integrity requirement.

> If the features provided by the vendor to meet this requirement cannot be exercised by the purchaser of the product, the vendor shall make available appropriate services to use the features as needed to meet the requirement. These services shall be available on an "on-demand" basis.

Support

Although desirable, it is not necessary for the validation mechanisms for hardware/firmware features to be directly accessible to the end-user. For example, the diagnostics may be designed for use of engineers who are experts on the product's hardware implementation, and it may be desirable, for the protection of proprietary information about the hardware design, to reserve those diagnostics to vendor personnel.

It is desirable, but not required, that at least some diagnostics be usable during normal product operation, and that diagnostics be performed automatically during initial system startup.

I-0170 Functional tests required for object reuse

This interpretation is effective 1994-04-18 and applies to **Test Documentation**, *classes C2, B1, B2, B3, and A1.*

The following interprets the requirement that "The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB."

> TCB interface(s) that allow manipulation and review of the contents of a subject's address space and of other resources available at the TCB interface (storage and named objects, devices) shall have functional tests included in the vendor test suite to supplement the analysis for object reuse.

Support

This interpretation starts at C2, even though the testing requirement words begin at C1, because the object reuse requirement starts at C2.

For there to be a threat of residual data, unprivileged interfaces must exist to manipulate or review the resources, including the subjects's address space. Those interfaces must be tested, although the analysis for residual data is also required and probably at least as effective.

I-0172 Audit of imminent security violations

This interpretation is effective 1994-04-19 and applies to **Audit**, *classes B3 and A1.*

The following interprets the requirement that "The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded..."

> Audit of imminent violations is required only for actions that may lead to an actual violation (i.e., multiple failed login attempts, excessive use of identified auditable covert channels). The threshold for notification of the security administrator may be either settable by an administrator or fixed by the vendor. There shall be an immediate notification mechanism included with the product (e.g., a message to an identified terminal, a red light as part of the hardware), and the TFM shall describe how the security administrator can monitor this mechanism.

Support

Both repeated login attempts and excessive use of covert channels (where excessive is defined as over the threshold for normal processing) are situations where protected data is likely to be released, unlike repeated attempts to access a file where the last attempt will not succeed if the first attempt did not.

The threshold for notification would best be done by a combination of vendor-fixed ranges and system administrator-settable values. In most cases the vendor understands more about covert channel violations than system administrators. Of course, the vendor should allow the least disruptive action to be a site-settable option and should make the setting of thresholds as dynamic as the product's market demands.

Notification of imminent violation is relatively easy with large main-frame operations, where there are usually operators, system administrators, and sometimes security officers on the job at all times. In the current workstation environment, the situation is very different.

I-0192 Interface manuals as design documentation

This interpretation is effective 1994-04-19 and applies to **Design Documentation**, *classes C1, C2, B1, B2, B3, and A1.*

The following interprets the requirement that "Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB."

> Interface-reference manuals (e.g., UNIX manual pages) are not sufficient, by themselves, as TCB design documentation.

Support

As example interface-reference manuals, UNIX manual pages include the name of the commands, a summary of their use, an interface-level description of their actions, the files built into the program, diagnostics, known bugs and deficiencies, and pointers to related commands.

The internal implementation of policy-enforcing subsystems must be documented and interface-reference manuals do not provide this. At C1-B1, subsystems that are not policy enforcing need documentation of only their interfaces. Interface-reference manuals may supply this for those subsystems that are part of the TCB interface. They do not document the interfaces of internal TCB subsystems.

I-0193 Standard system books as design documentation

This interpretation is effective 1993-10-20 and applies to **Design Documentation**, *classes C1, C2, B1, B2, B3, and A1.*

See related interpretation "**I-0192** Interface manuals as design documentation".

The following interprets the requirement that "Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB".

> Books describing the design and implementation of a system used as the basis for a trusted system, but which are inaccurate or incomplete for the trusted system implementation, are not sufficient as design documentation. Such books may partially fulfill the requirement if additional documentation provides a complete description of all differences between the book's description and the actual system implementation, including a satisfactory description of any parts of the TCB not described in the book(s).

Support

Such books as "The Design and Implementation of the 4.3 BSD UNIX Operating System" by Leffler, McKusick, Karels and Quarterman and "The Design of the UNIX Operating System" by Bach have been proposed as design documentation. However, these books do not cover all of the TCB of an actual trusted system, do not discuss the TCB concept or definition, and do not describe the details of the security policies implemented by an actual trusted system. In such books little coverage exists for software outside the kernel, while in actual systems much of the TCB is in non-kernel software. Note that the level of detail in these example books is in excess of that necessary to meet the C1-B1 class of this aspect of the requirement for non-policy enforcing parts of the kernel.

The effort to supplement such books with the necessary corrections and additional information is likely to exceed the effort needed to just write the required design documentation for the implemented system. Coherent documentation also enhances the reader's understanding of the system and makes both evaluation and maintenance easier.

Complete standard books written to describe the implemented trusted system would, of course, be acceptable

as design documentation and would have to be supplemented as the product went through revisions during RAMP.

I-0213 Administrator interface is part of TCB

This interpretation is effective 1995-01-12 and applies to **System Architecture**, *classes C2, B1, B2, B3, and A1.*

This interpretation affects the TFM.

The following interprets the requirement at C2 that "The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements."

> Those components of the product that provide the interfaces required for performing administrative actions shall be considered TCB components.
>
> The "administrative actions" to which this interpretation applies shall be those that are defined in the TFM to be performed by administrative personnel (e.g., operators, system administrators, system security officers) while the product is in its secure operational state. The TFM shall clearly identify which mechanisms are, and which are not, acceptable for performing each administrative action.

Impact

Treatment of TCB components that provide administrative interfaces has been inconsistent in previous evaluations, but for most products the impact of this interpretation is believed to be negligible.

Support

As used above, "administrative actions" are those that are performed by administrative personnel (e.g., operators, administrators, system security officers) while the product is in its secure operational state. It does not include activities such as initial configuration, failure recovery, and so on.

All of the TCB must meet the TCSEC requirements. The mechanisms used by administrators are perhaps the most important parts of the TCB. In many products the administrator, through these mechanisms, creates or modifies the security databases upon which the TCB depends for its correct enforcement of the security policy. Thus, any program that is (as part of a procedure defined in the TFM) executed by an administrator and that (A) is itself privileged (e.g., has a MAC exempt privilege), (B) becomes privileged when run in an administrator-controlled privileged environment (e.g., UNIX "rm" executed by a process running as owner "root"), or (C) is used to update a security database in a standard MAC and DAC protected object (e.g., "emacs" used to update the user file), is part of the TCB.

The TFM becomes an important part of the definition of the administrative portions of the TCB. It advises administrators to use specific commands or programs in specific ways to perform normal administrative procedures, and not to use anything else. At C2-B1, where administrative roles may not be well defined, the TFM is vitally important and must be followed by the administrator. Programs or commands that the

TFM specifies are to be run with privilege or just with administrative identities are part of the TCB. Those commands or programs that are not specified for use by administrators and that untrusted users cannot run with privilege are not part of the TCB. At B2, administrative interfaces are better defined and separated in function, but the TFM specification of administrative interfaces still helps determine the TCB. At B3, the TCB restricts administrators from using the wrong interfaces to execute security relevant administrative functions.

I-0222 Passwords not acceptable for DAC

This interpretation is effective 1994-12-05 and applies to **Discretionary Access Control**, *classes C1, C2, B1, B2, B3, and A1.*

The following interprets the requirement that "The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both."

> The TCB shall not depend solely on passwords as an access control mechanism. If passwords are employed as part of an access control mechanism, they shall not be considered sufficient to satisfy any aspect of the DAC requirement.

Support

This is a restatement of Formal Interpretation C1-CI-06-84, and extends it to include C1.

Discretionary access controls may be implemented by various mechanisms (e.g., access control lists, groups). However, the selected mechanism must allow the TCB to check the users' access by identity (i.e., named individuals) or by group identity (i.e., defined groups). Password-based access control does not provide this capability whether the password is on the object or on a group, and, therefore, was not included in the examples of suitable enforcement mechanisms in the requirement.

As is covered by the I&A requirement, passwords may be used for the authentication of the user's identity at login or at a change in identity, not for access control decisions.

It is acceptable for a product to provide passwords on objects along with a non-password access control mechanism. However, because of the difficulties in using and controlling passwords in a secure manner, it is preferable not to employ passwords as an access control mechanism.

I-0239 Subject access revocation after change in user clearance

This interpretation is effective 1994-04-19 and applies to **Mandatory Access Control**, *classes B1, B2, B3, and A1.*

This interpretation affects the TFM.

See related interpretations "**I-0001** Delayed enforcement of authorization change", "**I-0002** Delayed revocation of DAC access", "**I-0003** Access validation after object label change", and "**I-0004** Enforcement of audit settings consistent with protection goals".

The following interprets all of the MAC requirement.

> If a system allows an administrator to change the MAC subject security database values (e.g., the clearance range for a user), the TFM shall describe how the change can be accomplished while still enforcing the system's MAC policy as specified in the security database. A procedure followed by an administrator is sufficient for the enforcement of the policy if it is easy to ensure that the values in the database control all subsequent actions (e.g., read from a file, no batch jobs run under the wrong clearance). If the procedure is too complicated, TCB enforcement shall be required.

Impact

May have some impact.

Support

Only a system administrator should be capable of changing a user's clearance range. Complexities lie in handling subjects queued for later execution (e.g., batch jobs). System administrators are supposed to understand the product and the system security policy that is being enforced. Procedural methods of ensuring that no relevant subjects are active while a user's clearance is being changed may not be difficult. For example, the procedure could be that the administrator must always lock a user's account and make sure that no subjects are active or queued under that user's identification before changing the user's clearance. A more supportive TCB implementation would either inform the system administrator if the change in the user's range would affect a current subject (e.g., the subject's current label is not within the new clearance range), or provide immediate enforcement of the new range. Batch jobs may be more difficult to locate, and a TCB mechanism that checks MAC and DAC attributes before executing batch jobs makes an administrative procedure unnecessary.

I-0240 Passwords may be used for card input

This interpretation is effective 1993-10-20 and applies to **Identification and Authentication**, *classes C1, C2, B1, B2, B3, and A1.*

The following interprets the requirement that "Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user."

> The card input of batch jobs may contain human-readable user passwords. The TFM and the SFUG for the product shall explain the risks in placing passwords on card input and shall suggest procedures to mitigate that risk.

Support

Passwords on cards are not under the control of the TCB. It is possible to define procedures (e.g., that there be one person in the card reader room at a time, who feeds the card reader personally and then removes the cards) to prevent unencrypted passwords that are punched into cards from being read by another user. The FER should emphasize the high risk of this type of batch job input.

I-0244 Flexibility in packaging SFUG

This interpretation is effective 1993-10-20 and applies to **Security Features User's Guide**, *classes C1, C2, B1, B2, B3, and A1.*

This interpretation affects the SFUG.

See related interpretation "**I-0069** Flexibility in packaging TFM".

The following interprets the entire SFUG requirement.

> All SFUG documentation shall be in a form that system administrators and users can read at the time that an understanding of the topics covered is needed to use the system in a secure manner (e.g, it shall not be required that the user login in order to read instructions about how to login). The documents or portions of documents that make up the SFUG shall be precisely identified. There are no further restrictions on the packaging (one document, several documents, parts of several documents) or delivery (hardcopy, online) of the SFUG.

Support

Although the literal words of the SFUG requirement refer to a single section, chapter, or manual, this is not intended to restrict unduly the vendor's options in packaging the information, as long as it is clearly and concisely identified. The SFUG and TFM may be packaged in the same document, if the appropriate chapters are identified for each requirement (although in most systems untrusted users do not need access to the TFM). Some systems (e.g., certain network components) have no interface for untrusted users and therefore no SFUG. All of the SFUG can be online, except for information needed before an online status can be achieved.

Although this interpretation does not restrict the packaging of these documents, we do expect a coherent document, or documents, either in the form of one or two documents or in the form of a "road map" that clearly points to the sections of the SFUG in several documents.

I-0253 Default page marking format

This interpretation is effective 1994-11-16 and applies to **Labeling Human Readable Output**, *classes B1, B2, B3, and A1.*

See related interpretations "**I-0039** Multilevel printers and page labeling" and "**I-0040** Requirements for overwrite label capability".

The following interprets the requirement that "The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page."

> When the TCB applies default markings on printed output, at least one line shall be reserved for the top and bottom labels and those page labels shall be clearly recognizable. Labels that are in the same font (size and type) as the adjacent user data and are not separated by white space or some other delimiter (e.g., boxes), are not sufficiently distinct. Page labels shall be positioned to ensure that alignment of the paper within customary tolerance cannot result in the loss of the labels at the top or bottom of the page. All user output on the page shall be located below the top label and above the bottom label. Each top and bottom page marking shall indicate if the human readable representation of the label does not fit in the reserved area by printing as much of the label as possible followed by some indication that the whole label was not printed (e.g., label - (more)).

Impact

Some evaluated systems do not currently meet this requirement.

Support

The default markings must, as accurately as possible, indicate the sensitivity of the output. When they indicate that the label does not fit in the reserved area, a suitable complete label can be found on the banner page. Different forms of page labeling such as diagonal overprinting may also be used, but they cannot act as a replacement for the top and bottom page labels.

If page labels are so close to the top and bottom of the page that often a printer operator cannot adjust the paper so that the top and bottom labels are on the same page or, during use, the printer does not maintain the correct alignment, the page labels are not acceptable.

DoD and government standards such as DoD 5220.22, Army Regulation 380-5, and DOE 5635.1A all require page labels to be conspicuous and some give specific instructions on the size of the letters and the separation between labels and user test.

I-0254 UNIX-style manual pages as DTLS

This interpretation is effective 1994-12-05 and applies to **Design Specification and Verification**, *classes B2, B3, and A1.*

The following interprets the requirement that "A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and

effects. It shall be shown to be an accurate description of the TCB interface."

> When complete and accurate, documentation in the style of UNIX "manual pages" is sufficient to satisfy the requirement for a DTLS.

Support

Although UNIX "manual pages" are, in general, TCB interface documentation, they usually not sufficiently correct or complete to serve as a DTLS. Such documentation is often not entirely accurate and does not describe all exceptions, error messages, and effects (in particular, audit messages); in particular, trusted process descriptions are often inadequate. Also, such documentation rarely describes the complete TCB interface, for example lacking descriptions of the unprivileged instruction set or protocol interfaces. Examples of common omissions include the following:

- error returns that are common to many interfaces, such as access errors encountered in resolving pathnames
- error returns that result from internal errors or table overflows
- the order in which errors are detected and returned
- the audit messages generated as a result of success or failure of an operation
- complete descriptions of all options and arguments to trusted processes (such as "lp")
- complete descriptions of the environmental "parameters" to trusted processes, e.g., environment variables, temporary files
- complete descriptions of protocol-based and message-based interfaces, such as are commonly present in BSD UNIX-based systems for printer queue manipulation, remote execution, and so on.

I-0275 Single-level printers and page labeling

This interpretation is effective 1993-10-20 and applies to **Labeling Human Readable Output**, *classes B1, B2, B3, and A1.*

See related interpretation "**I-0039** Multilevel printers and page labeling".

The following interprets the requirements that "The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page ..."

> If a printer has been designated single-level (i.e., administrative intervention is required to change the TCB's understanding of the label of the printer and labels are not placed on the printed output by the TCB), it is acceptable to ensure that output is properly marked on the banner pages and

at the top and bottom of each page by administratively controlled, procedural means (e.g., use pre-marked paper, stamp each page after the output is removed from the printer). The TFM shall describe how the product can facilitate the procedural enforcement of labeling output from single-level printers.

Impact

This reverses previous guidance and allows procedural enforcement of labels for single-level printers.

Support

DoD regulations (DoD 5200.1R) specify that procedural means such as preprinted paper can be at least as trustworthy as TCB-produced markings for single-level printers.

I-0285 CM comparison source or object?

This interpretation is effective 1994-04-19 and applies to **Configuration Management**, *classes B2, B3, and A1.*

The following interprets the B2 requirement that "Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the version of the TCB." Also interpreted is the A1 change that "Also available shall be tools, maintained under strict configuration control, ..."

The tools and procedures used in comparing two versions of the TCB shall be able to show a mapping between the design descriptions of intended changes to the TCB and the actual changes in the compared TCB versions. The comparison tools shall operate on either or both of the TCB source code and TCB object code.

Support

The critical aspect of this requirement is the demonstration that the intended changes have been carried out, and therefore that a mapping between the design and the changes be demonstrated. While, in principle, such a mapping can be shown for either source code or object code, such a mapping to object code appears far more difficult than for source code, and its feasibility has not been demonstrated.

This requirement begins at B2, where analysis of the system is at the source code level and the comparison of versions of the TCB is at most a check on configuration management procedures, not a means for detecting attempts by development personnel to introduce trap doors in the object code. Even at A1, comparison of object code versions is not required, since without a requirement to ensure that the compiler generated the correct object code for the original version, a comparison of new object code with the original version does not increase assurance that there are no compiler-generated trap doors.

I-0286 Auditing unadvertised TCB interfaces

This interpretation is effective 1994-04-18 and applies to **Audit**, *classes C2, B1, B2, B3, and A1.*

The following interprets the requirement that "The TCB shall be able to record the following types of events: ... and other security-relevant events".

> The TCB shall be capable of auditing all security-relevant events that can occur during the operation of the evaluated configuration, including events that may result from the use of TCB interfaces not advertised for general use.

Impact

Additional auditing may be required for unadvertised interfaces in some products, but this largely formalizes current evaluation practice.

Support

An advertised interface is one that is described by the TFM, SFUG, or other user documentation. However, a product may also include other interfaces that are not intended for general use and that are not covered by the product's distributed documentation, but that could be invoked by non-TCB programs. Nonetheless, even unadvertised interfaces must be documented in the product's design documentation, and are considered in the evaluation.

I-0288 Actions allowed before I&A

This interpretation is effective 1994-04-18 and applies to **Identification and Authentication**, *classes C1, C2, B1, B2, B3, and A1.*

The following interprets the requirement that "The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate."

> Prior to having been identified and authenticated by the TCB, a user communicating with the TCB may be allowed to perform only those actions that would not require TCB mediation.

Support

User actions before identification and authentication should not require access to protected objects, and they should not be visible to or affected by untrusted subjects. These actions need not be auditable.

TCB actions that would be acceptable before I&A include displaying a login banner, responding to help requests with help information, and providing a mechanism to request assistance from a trusted user. Actions

that would not be acceptable include access to any file system object and sending or receiving messages from or to other users or terminals.

I-0312 Set-ID and the DAC requirement

This interpretation is effective 1994-04-19 and applies to **Discretionary Access Control**, *classes C1, C2, B1, B2, B3, and A1.*

The following interprets the entire DAC requirement and applies to products that implement a mechanism similar to the set-user ID/set-group ID (set-ID) mechanism defined in IEEE Standard P1003.1.

> The set-ID mechanism can be part of an acceptable DAC implementation.

Support

DAC, as defined in the TCSEC requirements, is inherently susceptible to Trojan horse programs and, except for a few restrictions in the requirements, is a policy defined by the implementation. Therefore, the set-ID mechanism, although easily misused, is not inherently worse than DAC in general.

This interpretation applies to a specific set-ID implementation which requires positive action (creation of the set-user-ID program) by the user whose identity is being assumed. It would not apply, for example, to a very different TCB interface that says "assume an arbitrary identity" without restriction or consent.

It is recommended that the set-ID mechanism include some provisions to make it stronger. The TCB should turn off the set-ID bits when an executable file is modified. In systems that implement a trusted path, the bits should be settable only through the trusted path. However, the strength of the mechanism still depends on programs avoiding many other possible errors, and the SFUG should include guidance on the mechanism's safe use.

I-0315 Restricted to trusted administrative interface

This interpretation is effective 1995-01-12 and applies to **Trusted Facility Management**, *classes B3 and A1.*

This interpretation affects the TFM.

The following interprets the requirement that "The TCB shall support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. ... Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively."

> The interfaces specified in the TFM for performing operator, administrator, and security administrator functions shall be the only interfaces available for performing those functions while the product is in its secure operational state.

Support

The definition of TCB in the back of the TCSEC states that "The ability of a TCB to correctly enforce a unified security policy over a system depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters related to the security policy." The TCB makes security decisions based upon information that has been provided by the operators and administrators; therefore, a critical part of the TCB is the part that implements operator and security administrator functions. To provide the needed assurance at B3-A1, the TCB interfaces provided for operators and administrators restrict the actions that they can perform with privilege.

The TCB interfaces for operators and administrators are subject to configuration management, design documentation, design specification and verification, security testing, system architecture and trusted distribution requirements. These interfaces also affect the security enforcing mechanisms in well defined ways (e.g., auditing, DAC, MAC, and trusted path). Covert channel analysis is applied only to untrusted user interfaces, since privileged users must be assumed not to be malicious. Trojan Horse attacks on administrators are prevented by the administrators' use of the supplied TCB interfaces for administrative work, and their use of the trusted path wherever needed to assure communication with the TCB.

Appendix A
Previous Interpretations

This appendix includes all of the formal interpretations created prior to the establishment of the Interpretations Working Group (IWG). They are listed in chronological order as they appear on the Eval_Announcements forum on Dockmaster. Each interpretation is named with the "subject" that identifies it on the forum and with the report number that National Security Agency (NSA) uses to track these formalized statements. Each interpretation includes a statement of the criterion to which it applies and the accepted interpretation, as it was originally written. Additionally, statements regarding specific applications, alternate possible interpretations, issues, and rationale are included for reader convenience. If an interpretation has been superseded by an interpretation generated under the new (IWG) process, the name and number of the superseding interpretation is given preceding the statement of the criterion.

Security Testing - Interpretation (Report No. C1-CI-01-83)

Criterion:

3.1.3.2.1 Security Testing (B1)

> "... as well as to assure that no user (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users."

Specific Application:

Version 1.0 of the SCOMP cannot always guarantee response to users. It has been consistently demonstrated that the system can be caused to enter a state such that it will no longer respond to user commands issued from any terminal.

The question that has been discussed is whether or not the rating given to version 1.0 of the SCOMP should be affected by it's tenderness to user inputs.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. Crashing the system, i.e. causing the system to enter a state such that it can no longer respond to user requests without operator intervention, is a violation of the Criteria and should therefore affect the rating given.

2. The Criteria does not require robustness in a system and therefore a rating should not be affected due to lack of robustness. However, one of the objectives of the testing required by the Criteria is to note the robustness of a system.

Issues:

1. It is difficult to define what a "crash" really is and therefore the venders cannot be required to make a machine that is "crash" proof.
2. Does security require that a system be able to provide the proper information to the proper user or is security simply restraining users from receiving information that does not pertain to them?

Rationale:

At the present time, there is no widely accepted definition for denial-of-service. Therefore, it would be very difficult to evaluate a system in this area. It is thought best that, until this problem is resolved, this issue will not adversely affect the rating given to any system.

Accepted Interpretation:

It is accepted that the rating will not be affected by the denial of service issue until a working definition for denial of service is found. However, comments about the issue as it pertains to the system in question may be included in the final report.

16 May 1983

Identification and Authentication - Interpretation (Report No. C1-CI-02-83)

Criterion:

2.1.2.1 Identification and Authentication (C1)

> "The TCB must require users to identify themselves to the TCB before beginning to perform any other actions that the TCB is expected to mediate. It must provide some form of TCB-enforced and protected authentication (e.g., passwords) for authenticating the user's identity. The TCB must protect authentication data so that it cannot be acquired by an unauthorized user."

2.2.2.1 Identification and Authentication (C2)

> "... The TCB must be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB must also provide the capability of associating this identity with all auditable actions taken by that individual."

Specific Application:

RACF has some problem meeting the letter of the above criteria in respect to the device commonly known as the "operator's console."

Possible Interpretations:

We recognize that the "operator's console" is typically protected by the same physical mechanisms as the hardware itself. Therefore, slightly less stringent authentication is necessary to insure adequate security than would be necessary at a user's terminal. The problem arises in that the criterion does not recognize the "operator's console" as being different from a user terminal.

The following are possible interpretations:

1. We can define the "operator's console" and treat it as an exception.

2. The criterion can be interpreted literally and require authentication of those using the console.

3. It can be argued that the physical security provides the necessary authentication.

Issues:

1. Many systems including those above assume the "operator's console" has adequate physical protection and therefore user authentication is not necessary.

2. The idea of an "operator's console" is a hard thing to clearly define. We propose the following definition:

   > Operator's Console - any terminal, device or set of switches used only for ADP system operational purposes and having the same physical access requirements as the ADP system itself.

3. If we accept the argument that the physical security provides sufficient authentication, how much more will we depend on physical security in other areas?

Rationale:

It is expected that most C level systems will not be especially robust in terms of security. One of the common historical examples of this lack of robustness is the misconception that operator's need to be all powerful. In the past it has been felt that since operator's have acccess to the hardware itself then software controls would not provide any worthwhile protection. Since a high degree of trust can not be placed in C level systems, non-TCB means of protection must be in place to adequately protect the information. Therefore, it does not seem to adversely affect the trustworthiness of the system to allow the operator's console to be an exception to this criterion. However, at the B and A levels we would expect a more robust mechanism to be in place for the operator's console.

Accepted Interpretation:

The accepted interpretation is that the "operator's console" will be defined as stated above and will be considered an exception to the authentication and individual accountability requirements provided that it is protected by the same physical security mechanisms that protect the ADP system itself.

16 May 83

Audit - Interpretation (Report No. C1-CI-01-84)

This interpretation has been superseded by "**I-0006** Audit of user-id for invalid login."

Criterion:

2.2.2.2 Audit (C2)

> "... The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, ... For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event."

Specific Application:

The SCOMP does not record the character string in the audit record. Instead all user names are translated to a number (user-id) and the user-id is stored in the audit record. In the case of a user not entering a valid user name, (i.e., a string that does not correspond to a valid user-id), the SCOMP leaves the user-id portion of the record blank.

Possible Interpretations:

The following are proposed interpretations of the above section of the Criteria:

1. The use of identification and authentication mechanisms is the equivalent of attempting to login. Therefore, any attempt to login, whether or not a valid user-id is supplied must produce an audit record. This audit record must contain the user-id if a valid user-id was supplied. If no valid user-id was supplied then the characters entered at the terminal must be recorded.

2. The use of identification and authentication mechanisms is the equivalent of attempting to login. Therefore, any attempt to login, whether or not a valid user-id is supplied must produce an audit record. This audit record must contain the user-id if a valid user-id was supplied. If no valid user-id was supplied then the audit record need only contain the information that a failed login attempt has occured, and the other identifying information such as port/terminal number, date and time, etc.

Issues:

1. Recording the character string entered by the user would make obvious to a security administrator when someone is trying certain methods of guessing user-ids (AAAA, AAAB, AAAC, ...).

2. It is obvious that the "user" cannot be identified, as required by the Criteria, since the proper authentication has not been provided. Therefore, the next best thing is to record what the user provided as identification in the audit record.

3. Recording invalid user-ids is a possible security exposure. A legitimate user may devulge his password by a common scenario where the user becomes confused and enters his password as a user-id after a failed attempt to login with his correct user-id.

4. Asking the vendors to record the actual characters that are entered is an implementation detail and should not be included in an interpretation of the Criteria.

Rationale:

It is agreed that the "user" can not be identified when an invalid ID is entered. Therefore, the decision that needs to be made is whether the character string that was entered as an ID needs to be recorded in the audit log. It was decided that, although recording the character string can give the security administrator a clue as to how a potential penetrator is trying to get into his system, the benefits of this are outweighed by the possible security exposure that may result when a user becomes confused and enters his password in place of his ID immediately after mistyping his password on a previous attempt. It was also noted that the Criteria does not specify implementation details and that these should not be considered in Criteria interpretations.

Accepted Interpretation:

It is accepted that the audit mechanism be required to produce a record on all login attempts. When a valid user-id is specified in the attempt, the audit record must have some means of identifying that user-id. In the case that no valid user-id is specified, the audit record should be generated indicating that a failed login attempt has occured. It is further recommended that the decision as to whether to record the character string supplied be left to the vendor.

15 June 1984

Security Testing - Interpretation (Report No. C1-CI-02-84)

Criterion:

4.1.3.2.1 Security Testing

> "This interpretation deals with security testing in general and is not intended as an interpretation of any specific words within the security testing requirement."

Specific Application:

In doing penetration testing on the SCOMP the question was raised as to the need to establish, through testing, the actual bandwidths for the known covert channels.

The question deals with issues internal to the penetration team and is not meant as a guide to vendors. The interpretation of this issue can be applied to all evaluations dealing with systems targeted from B2 through A1.

Possible Interpretations:

The following are proposed interpretations of the above section of the Criteria:

1. The security testing team must run tests to determine the actual bandwidths of known covert channels, (i.e., covert channels discovered through application of verification methodologies.)
2. The evaluation team should review the estimates of the bandwidths but need not run tests to verify those estimates.

Issues:

1. In most evaluations the time alloted to security testing is very limited. Since the channels are already known there is no sense in wasting time writing and running programs to determine actual bandwidths.
2. The evaluation will lose credibility if the actual bandwidths of known covert channels are not tested and someone else demonstrates that they are much higher than the vendor supplied estimates.
3. Testing the actual bandwidths of known covert channels will help support the findings produced by the verification work.

Rationale:

In evaluating commercial computer systems, the evaluation team has a limited amount of time that can be spent on the testing of that product. When a vendor measures or estimates the bandwidths of the known covert channels, worst case scenarios should be used. This should produce measurements or estimates of the maximum bandwidths. Therefore, the team need only assure themselves that the specifics are worst case and that the measurements and/or estimates have been performed correctly. It is envisioned that some time in the future, a flaw will be found in a system that wasn't uncovered during an evaluation. It is not expected that evaluations will uncover all design and implementation flaws in every system.

Accepted Interpretation:

It is accepted that the evaluation team will review the evidence provided by the vendor in terms of known covert channel bandwidths. The team will review the evidence to ensure that the bandwidth of each channel is correctly and accurately assessed such that the guidelines on covert channels can be applied. No actual

testing need be conducted if the team feels that the evidence presented is sufficient to meet the claims of the vendor.

15 June 1984

Audit - Interpretation (Report No. C1-CI-04-84)

Criterion:

2.2.2.2 Audit (C2)

> "... The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects and actions taken by computer operators and system administrators and/or system security officers."

3.1.2.2 Audit (B1)

> "... The TCB shall also be able to audit any override of human-readable output markings."

3.2.2.2 Audit (B2)

> "... The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels."

Specific Application:

This interpretation was prompted by a question from Honeywell during the evaluation of Multics. Their question deals with the fact that not every security-relevant event can be defined as one of those listed in the requirement(s). Is it necessary to audit these events? This interpretation deals with the wording of the Criteria and not any specific implementation detail of Multics.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. The Criteria specifies all actions/events that must be auditable. We should adhere to the words of the Criteria.
2. Implicit in the requirement is the ability to audit all security-relevant actions.

Issues:

1. If we strictly adhere to the words of the requirements, there will exist (in some systems) the ability for users to repeatedly take illegal actions without any type of audit record being generated.

2. The Criteria, in some areas, is not an all inclusive document and that is the reason for interpretations. This happens to be one of the areas where the Criteria does not fully specify what is required.

Rationale:

The list of events stated in the Criteria were intended to be a set of examples of what must be audited. Implicit in the audit requirement is the ability to audit all security-relevant events. Evidence in support of this is found in the short summary at the beginning of the class C2 section of the Criteria. It states here that "Systems in this class enforce a more finely grained discretionary access control than C1 systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation ..."

Accepted Interpretation:

The ability to audit all security-relevant actions and events must be present in order to pass the audit requirements at any level of the Criteria.

5 September 1984

Exportation to Multilevel Devices - Interpretation (Report No. C1-CI-05-84)

Criterion:

3.1.1.3.2.1 Exportation to Multilevel Devices (B1)

> "When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form)."

Specific Application:

CDC's NOS appears to have the capability to support multilevel tapes. Multilevel tapes are defined to be a single reel that contains information marked in such a way that the TCB can unambiguously, and accurately, read and write files of differing security levels. In other words, the TCB can "trust" the labels for PARTS of the reel rather than the current practice of only "trusting" the label of the entire reel.

NOS already has a trusted tape handler which is the most difficult facility to develop for the support of multi-level tapes. CDC claims that there is no room in the standard tape headers, be they ASCII standard or CDC standard, for security information and they do not want to implement multilevel tapes at the cost of the "portability" of these tapes.

One recommened solution to NOS's problem of implementing multilevel tapes is as follows:

The current tape headers do have a field that allows the tape to be uniquely identified. That identifier could be mapped to a trusted description of what is on that tape, including security levels of each file, and the TCB could use that description to make access control decisions. This description would reside in a special system disk "file" which only the system can access. The system will have to use privilege to read and write the "file" since it would simultaneously contain information at different security levels.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. The Criteria states that the the security label for an object exported to a multilevel device must reside on the same physical medium as that object. Or in other words, for every file that is exported to a multilevel tape, that file's security level must also physically reside on that tape.
2. If a "trusted" multilevel device can find a "trusted" pointer for a file or a collection of files that points to a "trusted" directory that reliably describes all files currently on that device, including reliable security labels, then the spirit, if not the words, of the requirement in the above section of the Criteria is met.

Issues:

1. Most systems do not store the actual word CONFIDENTIAL, SECRET, etc. with each file but rather store a bit pattern that represents a label that the system can recognize. NOS has this same capability with a unique pointer for every physical tape reel. This pointer can be mapped to a trusted system directory that can reliably describe all objects on that tape, including security levels.
2. The underlying objective behind a multilevel device is to insure that the TCB can reliably enforce mandatory access controls on all objects stored on that device. Or in the case of a multilevel tape, once dismounted and remounted, the TCB can reliably enforce mandatory access control on all objects stored on that reel. NOS appears to have the capability to meet this objective by mapping a unique pointer on all multilevel tape reels to a protected directory on a special system disk that can accurately supply the security level for all files stored on that reel. Since NOS possesses a trusted tape handler and only the system can access the protected directory, reliability is also insured.

Rationale:

The Criteria does not specify implementation details and is not meant to restrict design ideas. Therefore, if a system can implement the intent behind a feature of the Criteria in a trusted manner, that mechanism will be judged as satisfying the requirement of the Criteria. Even if the mechanism does not strictly adhere to the stated words of the Criteria.

Accepted Interpretation:

If multi-level tapes can be implemented in a trusted way without the object's actual label being stored on the same physical medium as the object, the Criteria requirement is satisfied.

5 September 1984

Discretionary Access Control - Interpretation (Report No. C1-CI-06-84)

Criterion:

2.2.1.1 Discretionary Access Control (C2)

> "... These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users."

Specific Application:

The Gould MPX-32 operating system uses self/group/public access controls. Users have no control over the group mechanism, they can not create groups. The knowledge of a password provides the ability to become a member of a group. There is no "list" of users that belong to any group on the system.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. If the system administrator constructs the super-set of all possible groups, it is possible to include and exclude down to the granularity of a single user. This is sufficient to satisfy this requirement. Any user with access to an object can eventually give away the information contained in that object. Therefore, it is not unreasonable to consider any user with access to an object as authorized to grant access to that object.
2. This implementation does not satisfy the requirement. Even with the super-set of all possible groups it is impossible to determine the membership of a group at any time. Membership in a group is defined as the knowledge of a password, therefore, use of the groups defined by the super-set can not be enforced. Also, access to an object should not authorize a user to in turn grant access to other users.

Issues:

1. Even if a system would support the number of groups needed to implement the super-set of the user set, most installations' system administrators would not create this super-set. Nor would they adjust

this super-set every time a user is added to or deleted from the system.

2. If the super-set did exist, users would need to memorize it and all the associated passwords (if the implementation is password based) in order to use it correctly. Few users, probably none, would do this.

3. A system with the above discussed "features" would never be used in a secure manner and should not be rated as being a system that is secure to the C2 level.

4. If this type of access control is allowed for systems at the C2 level, then these controls must also be judged as satisfying the B2 DAC requirements. At the B2 level, the requirements for system architecture become much more rigid. Do we really want to allow a B2 system to have group access control mechanisms? We require a much more strict architecture, why not access controls also?

Rationale:

The class C2 requirement for Discretionary Access Control specifies that only authorized users be able to permit access to an object to users who previously had no access. With a password-based mechanism this can not be enforced. Any user with access to the object can reveal the password to other users, thus granting access to the object. This violates the intent of this section of the requirement.

The intent of this section of the requirement is that some separate type of access to an object must be given by the owner of the object or the security administrator before any other user can permit access to that object by users not already possessing access permission.

Accepted Interpretation:

Discretionary Access Control mechanisms, where access is controlled solely by passwords, do not satisfy the C2 requirement for discretionary access control.

5 September 1984

Audit - Interpretation (Report No. C1-CI-07-84)

Criterion:

2.2.2.2 Audit (C2)

"... The TCB shall be able to record the following types of events: ..."

Interpretation C1-CI-04-84 indicates ALL security relevent actions and events must be audited.

3.2.2.2 Audit (B2)

> "... The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels."

Specific Application:

This interpretation was prompted by a question from a vendor in regard to the event "object not found." It is possible in their system to have several search paths which are traversed in looking for a file. If "object not found" is an auditable event then there might be several entries in the audit log for a file which is eventually found.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. "Object not found" must be audited at all levels. It can be a covert channel. It is also a security related event to catch someone "fishing" either in general or, as in some systems, to gain access to an object (allowed when the full path name is known) where access would be denied if the path name is not known.
2. At the C2 level, one is not interested in covert channels. Probing existence is often a legitimate user action. One would find a "fisherman" based on the access auditing of what was found. What about "wildcard" activities? To audit "object not found" would overwhelm the system with useless information (mainly the quality of the typists).

Issues:

1. If we strictly adhere to the previous interpretation "object not found" must be audited as being security related.
2. At any level some events are security related and some are not. At C2 "object not found" is not while at B2 it may be (i.e., at B2 it may be a covert channel).

Rationale:

For the B1 level and below, the fact that a user receives an error message of "object not found" is not a security relevant event. The message does not positively indicate a misuse of the system, it will most often be a benign mistake on the part of a user. However, at the B2 level and above this error message, as well as any other error message, could possibly be used to pass information in violation of the system's security policy.

Accepted Interpretation:

The ability to audit "object not found" is not required at the C2 or B1 level. It is required at the B2 level and above if it results in a covert channel.

19 December 1984

Device Labels - Interpretation (Report No. C1-CI-01-85)

This interpretation has been superseded by "**I-0007** Assigning device level range."

Criterion:

4.1.1.3.4 Device Labels

> "The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices."

Specific Application:

This interpretation fixes a grammatical error that was present in Criterion Interpretation C1-CI-03-84 that allowed the mis-interpretation of its intent. Capitalization shows what was added to clarify the intent of this interpretation.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. The assignment of device minimum and maximum levels need not be a system changeable parameter. If the device maximum level is system high and the device minimum level is system low then this implementation will meet the requirements of the Criteria.

2. The assignment of maximum and minimum device levels must be site changeable. The site should, at the very least, be able to specify the maximum and minimum security levels for each configured device at system generation time.

Issues:

1. There is no real security problem associated with leaving the minimum levels at system low. The only security risk occurs when the system allows information at too high a level to go to a terminal.

2. In a configuration where a machine is a part of a network it is important that the ports used to connect different machines restrict both the maximum level of information leaving the machine and the minimum level of information entering the machine. This is due to the fact that all machines on the network may not have the same levels for system high and system low.

Rationale:

If it was accepted that system high and system low be acceptable as the maximum and minimum device labels, then the requirement in the Criteria would have no meaning. It is considered fairly obvious that the requirement is for the maximum and minimum device labels, FOR EACH DEVICE, to be settable by the site that is using the system. IN OTHER WORDS, ALL DEVICES ARE REQUIRED TO POSSESS MINIMUM AND MAXIMUM DEVICE LABELS WHICH ARE SETTABLE TO VALUES OTHER THAN SYSTEM LOW AND SYSTEM HIGH RESPECTIVELY.

Accepted Interpretation:

The system must support both maximum and minimum security levels that can in some way be specified, FOR EACH DEVICE, by the site that uses the machine. These parameters need not be dynamic in that it is acceptable that they may only be changed at system generation time. If they can be changed dynamically, this function must be restricted to the security administrator only.

This Interpretation supersedes Report No. C1-CI-03-84, 11 January 1985.

Audit - Interpretation (Report No. C1-CI-02-85)

Criterion:

2.2.2.2 - 4.1.2.2 Audit (C2-A1)

> "... The ADP system administrator shall be able to selectively audit the actions of ..."

Specific Application:

The issue of what is meant by "selectively audit" was raised during the SCOMP and Multics evaluations and is now being put to paper.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. Selectively audit means that sufficient audit information is always recorded by the TCB to allow selection to be done post-audit using vendor supplied reduction tools.

2. Selectively audit means that only security administrator requested information is recorded by the TCB.

Issues:

1. If post-audit reduction is allowable, must the vendor supply the reduction tools. If so, what functionality must the tools possess? To what degree must the tools be trusted?

2. Interpretation 1 could lead to an overwhelming amount of audit data.

Rationale:

How a feature is implemented should not, and does not, affect the decision of whether the requirement is satisfied or not. Therefore, both of the possible interpretations are acceptable. Reduction tools need only possess the minimal functionality necessary to satisfy the requirements stated in the Criteria (i.e., audit based upon individual identity and/or object security level). If supplied to provide post-audit selectivity, reduction tools, while not necessarily a part of the TCB, must be maintained by the vendor under the same configuration control system as the remainder of the system.

Accepted Interpretation:

"Selectively audit" means that the audit mechanism must be sufficiently flexible for the system administrator to obtain information regarding system activity based upon a user's identity or upon object security level. Both of these capabilities must exist, the "or" is meant to allow the security administrator the decision to audit one or the other or both. Audit reduction tools, when supplied by the vendor, must be maintained under the same configuration control system as the remainder of the system.

11 January 1985

Discretionary Access Control - Interpretation (Report No. C1-CI-03-85)

This interpretation has been superseded by "**I-0020** DAC authority for assignment."

Criterion:

2.2.1.1 Discretionary Access Control (C2)

> "... The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both ... Access permission to an object by users not already possessing access permission shall only be assigned by authorized users."

Specific Application:

CA-Sentinel, a DOS/VSE security add-on package, uses authorization lists to implement discretionary access control. Each subject has, attached to it, a list of objects which it may access. A question was raised when it was discovered that only privileged users are authorized to specify and control sharing of objects. These privileged users are the system administrator (SA) and other individuals whom he designates as data security officers (DSO). Objects, when created, are publicly accessable. They are not protected until the SA or a DSO defines them to CA-Sentinel. Once the object is defined, a user may only access that object if the object's name has been inserted into his authorization profile by the SA or a DSO.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. Implicit in the requirement is the ability for every user to specify and control sharing of objects he creates. He must be included as an "authorized user" for those objects.
2. It is not necessary for the creator of an object to be able to control access to that object in order to satisfy the requirement.

Issues:

1. The Criteria does not state who should have the discretion in discretionary access control. In some environments, it is desirable to limit the control of ACLs to a few individuals.
2. Should not each user be able to control the access to objects he creates?
3. Does this mechanism really meet the intent of the Criteria?

Rationale:

The discretionary access control requirement does not specify who must have the ability to grant access to an object, it only requires that the discretionary security policy of the system shall be enforced. The Center should not mandate one particular implementation of discretionary security (that is, the one in which the creator of an object has the authority to grant access to that object). Therefore, it should not be necessary that creators of objects have the ability to specify and control sharing of those objects.

Also, there are many situations where an installation may not want every user to be able to modify the access control permissions for the objects that he may create. The academic world is a good example of this. It may be desired that students not have the ability to share work among themselves. Government and business may have the same requirement in some instances. It may be necessary for a person to create objects during the course of performing his job but he may not have the authority to release that information to others. Also, when a user creates data on an ADP system, that data becomes the property of the government agency or company for which that individual works. It is not unreasonable, therefore, to only permit a small number of authorized users to control the sharing of that data.

However, in other instances it may be desirable for the installation to let users do their own access control maintenence. Therefore, an installation settable option may be the best way of implementing this facet of discretionary access control.

Accepted Interpretation:

The discretionary access control requirement at the C2 level does not state whose discretion should be used. Therefore, it is not necessary for creators of objects to have the ability to specify and control sharing of those objects (i.e., it is not required that the creator of an object be included as an authorized user for that object due solely to the fact that he is the creator of the object).

15 January 1985

DAC by Default - Interpretation (Report No. C1-CI-03-86)

Criterion:

2.2.1.1 Discretionary Access Control (C2)

> "... The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access ..."

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. When an object is created, the TCB must ensure that no user, without proper authority, may access the object. The discretionary access control mechanism must provide defaults that can be set so that objects are protected by default; or, at object creation time, the system must require the user to specify what the access permissions for the object are to be before that object is accessible by any other users.
2. The TCB must ensure that protection for objects is available. This can be done by either enforcing a secure initial access permission on objects or by providing users with a mechanism by which they can secure objects after creation.

Issues:

1. The first of the possible interpretations is clearly the more secure. It does not depend upon users remembering to apply the correct access permissions on objects at some time after the objects are created. It also does not provide a window through which objects may be accessed before the user adjusts the access permissions.
2. The second of the two possible interpretations is not secure. It is subject to the possible vulnerabilities mentioned in Issue 1.

Rationale:

The Control Objective, Rationale, and Relationship to Policy sections of the Criteria (sections 5, 6, and 7) show that the intent of the Criteria is to support DoD policy in automated systems. DoD policy is clear in that access to information may only occur when the proper conditions are met (i.e., the mandatory and discretionary access policies are satisfied).

DoD policy for need-to-know controls is explicit in stating that access to information is not to be given without a determination of need-to-know. The desired handling of information is that at first, access to information is limited and then it tends to spread as more people acquire a need-to-know for the information. Information should not be publicly available BEFORE access controls can be applied.

The words in the requirement section for Discretionary Access Control are ambiguous in their attempt to state DoD policy. The requirement, as stated, may be interpreted differently by different people. However, this ambiguity in meaning was noticed soon after the Criteria was published; evaluation teams have, in almost all cases, required that vendors comply with the interpretation leading to the more secure implementation.

Since it is the intent of the Criteria to conform to DoD policy, and only the first of the two possible interpretations can achieve this goal, the first of the two possible interpretations will be required.

Accepted Interpretation:

A system, to pass the Discretionary Access Control requirements at the C2 level and higher, must provide protection by default for all objects at creation time. This may be done through the enforcing of a restrictive default access control on newly created objects or by requiring the user to explicitly specify the desired access controls on the object when he requests its creation. In either case, there shall be no window of vulnerability through which unauthorized access may be gained to newly created objects.

Posted: 24 October 1986

Server - Interpretation (Report No. C1-CI-02-86)

Criterion:

2.2.1.1 Discretionary Access Control (C2)

> "... Access permission to an object by users not already possessing access permission shall only be granted by authorized users."

2.2.2.1 Identification and Authentication (C2)

> "... The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual."

Specific Application:

An operating system allows the ability for a user to authenticate himself to the TCB and connect directly to another user's process, if the connecting userid has been specifically granted this access by an authorized user. If that is the case, the connection is allowed and the event is logged when the connection is made and when it is disconnected. This may be thought of as a type of interprocess communication in which two or more cooperating users may share the abilities of one process. The mechanism cannot function unless the owner of the target process has taken some specific action which allows this type of interprocess communication to occur.

Possible Interpretations:

1. Since the user has been specifically granted access to attach himself to the target user's process by some authorized user, this configuration is allowable.

2. Since the TCB cannot account for the actions of a user once he attaches to another user's process, individual accountability is not enforced, and this configuration is not allowable.

3. Accesses to objects which are granted to the "connectee" are potentially granted to the "connector" when he attaches to the "connectee's" process. This is in conflict with the C2 DAC requirement.

4. If a user wishes to attach to his own process, this violates no accountability or DAC requirements, and should be allowed.

5. The mechanism is a form of DAC in which the target process, a subject, is the entity to which the control is applied. There are no vulnerabilities here which are not inherent in any DAC mechanism; therefore the configuration is allowable.

Rationale:

This facility can be thought of as a type of server mechanism. Any authorized user can connect to the server process, do whatever the server process allows them to do, and be held to some measure of accountability for the actions of the server process. To enforce this accountability, all connections made via this mechanism must be auditable at their initiation. Identification and authentication are required before the mechanism can be used. Any ability that could be provided by this mechanism to subvert DAC can be easily replicated using other mechanisms; therefore, as long as an authorized user must specifically allow another user access to connect to his process, system security policy is not violated. It should be noted that this refers to user processes only; servers which are part of the TCB, such as print spoolers, etc. are not included in this interpretation.

Accepted Interpretation:

The configuration is allowed as described above. If users of the ADP system are authenticated and have been authorized the ability to connect to another user's process, then DAC is not compromised, provided that the establishment of the path is auditable. In a B1 or higher level system, mandatory flow policies of the system must also be enforced.

Posted: 28 October 1986

Operator Log-on - Interpretation (Report No. C1-CI-04-86)

Criterion:

2.1.2.1 Identification and Authentication (C1)

> "The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. It must provide some form of TCB-enforced and protected authentication (e.g., passwords for authenticating the user's identity. The TCB must protect authentication data so that it cannot be acquired by an unauthorized user."

2.2.2.1 Identification and Authentication (C2)

> "... The TCB must be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB must also provide the capability of associating this identity with all auditable actions taken by that individual."

3.1.2.1 Identification and Authentication (B1)

> "The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity and to determine the security level and authorizations of subjects that may be created to act on behalf of the individual users. The TCB shall protect authentication data so that ..."

Specific Application:

The Identification and Authentication requirements are relatively clear when applied to regular system users, but uncertainties have persisted as to whether or not computer operators need to identify and authenticate themselves prior to gaining access to any system resources. Such ambiguity only exists with regard to systems of class B1 and above since Criteria interpretation C1-CI-02-83, issued May 1983, provides that operators of C1 and C2 systems need not identify and authenticate themselves using a mechanism under the control of the TCB. The purpose of this interpretation is to resolve the issue for those systems at and above the B1 level.

Possible Interpretations:

We recognize that the "operator's console" is typically protected by the same physical and procedural mechanisms as those applied to protect the system hardware itself. Therefore, these mechanisms may provide an adequate means of identifying and authenticating computer operators in lieu of TCB internal controls such as user IDs and passwords.

The problem arises in that the Criteria does not recognize the "operator's console" as being different from a user terminal located outside a physically-protected perimeter. The following are possible interpretations:

1. The requirements for user identification and authentication can be literally interpreted as to require each user to identify and authenticate himself to the system before performing any actions which would be mediated by the TCB. This would require each operator to identify and authenticate himself prior to taking such actions on the system. This interpretation would apply to all operator consoles regardless of physical location.

2. The physical and procedural controls usually applied to the computer system, TCB, and operator consoles are sufficient to ensure adequate identification and authentication of each computer operator. This form of user identification and authentication would not enable the TCB to trace operator actions to an individual operator. However, with proper recording of personnel admittance to the operator console area by mechanisms external to the TCB, a mapping of operator actions to an operator(s) is attainable.

Issues:

1. Many systems assume that the "operator's console" has adequate physical protection and therefore user identification and authentication is attained through the implementation of both physical and procedural controls.

2. To provide better clarification of what is meant by the term "operator's console," this definition is proposed:

   > Operator's Console - That device(s) that the operating system recognizes (as a result of hardware configuration) as a special device from which system operators perform their duties. This device must be protected by the same, or equivalent, physical protection mechanisms that protect the TCB hardware.

3. If it is accepted that physical and procedural controls can provide a sufficient means of user identification and authentication, how are remote operator terminals to be addressed?

4. Under the definition of "user," stated in the DOD Trusted Computer System Evaluation Criteria, computer operators would be considered as computer system users. Whether or not this definition is applied, operator actions must be audited at class C2 and above. The C2 and above requirement for user identification and authentication requires that the TCB must be able to uniquely identify those individuals whose actions are auditable. How will this requirement be met if individual operators are not identified and authenticated via a TCB mechanism ?

Rationale:

In the past, it has been felt that since operators have access to the hardware itself, then software controls would not provide any worthwhile protection. Since only a low level of assurance exists in C1, C2, and B1 systems, non-TCB means of protection must often be in place to adequately protect the information stored in these systems. Therefore, it does not seem to adversely affect the trustworthiness of the system to allow the operator's console to be an exception to the identification/ authentication criterion.

At and above the B2 level, the Criteria requires that the principle of least privilege be enforced. To meet this requirement, operators and their actions must be uniquely identified by the TCB.

Accepted Interpretation:

The accepted interpretation is that the "operator's console" will be defined as stated above and will be considered an exception to the C1, C2, and B1 identification and authentication requirements. This definition supercedes that found in criteria interpretation C1-CI-02-83. The key to this revised definition is the special status of the console, and the physical protection that must be provided. Those consoles outside the physical perimeter of the computer room must be protected by the same physical and procedural mechanisms as the system hardware itself, or must require the use of an identification and authentication mechanism under the control of the TCB.

To meet the various audit requirements, if multiple operator's consoles are used, the TCB must generate an audit record that identifies from which particular console the auditable event originated. In addition, the trusted facility manual must explain that a log should be maintained of who had access to any particular operator's console at any particular time. Even if only one console is available, such a record is necessary to trace specific events to specific individuals.

The exception to identification/authentication requirements provided by this interpretation does not extend to B2, B3, or A1 systems. Computer operators of these higher level systems must individually identify and authenticate themselves by means of a mechanism under the control of the TCB.

Posted: 11 December 1986

System Architecture - Interpretation (Report No. C1-CI-04-85)

Criterion:

3.1.3.1.1 System Architecture (B1)

> "... The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its source code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements."

Specific Application:

In past evaluations, computer systems offering two state architectures supported such by means of software and hardware controls. Systems exist which attempt to maintain a two state architecture primarily through the implementation of software mechanisms.

Process isolation is provided by a combination of hardware and software mechanisms. The hardware component enforces those addressing restrictions imposed by the software.

Possible Interpretations:

1. The words of the Criteria do not specify that TCB and user isolation be provided by a hardware-based architecture. Nor does the Criteria require that process isolation be supported by any specific hardware or software implementation. Therefore, a software architecture, if properly implemented, would satisfy the B1 level System Architecture requirements.

2. Implicit in the requirements for System Architecture is the understanding that user separation and two-state controls be implemented in hardware so that a greater degree of assurance would be provided. Given this interpretation, an architecture based primarily on software would not meet System Architecture requirements at the B1 level.

3. A software-based architecture can provide as much assurance as those implemented in hardware. Given this position, software-based architectures would meet B1 level System Architecture.

Rationale:

Hardware receives information from software, and based on that input it determines what actions are necessary. Therefore, hardware is as trusted as the software providing the input. Strictly software-based architectures can provide the level of assurance required to meet the C1-B1 level requirements for System Architecture.

Accepted Interpretation:

Software-based architectures are able to provide process separation and a two state architecture with sufficient assurance to meet the B1 level requirements for System Architecture. Simply because a two-state architecture is provided and maintained primarily by software should not lead to the assumption of its being less secure than hardware in implementing security features.

Posted: 11 March 1987

Discretionary Access Control - Interpretation (Report No. C1-CI-01-86)

Criterion:

3.2.2.1.1 - 3.3.2.1.1 Trusted Path (B2-B3)

> "The TCB shall support a trusted communication path between itself and users for use when a positive TCB-to-user connection is required (e.g., login, change subject security level). Communications via this trusted path shall be activated exclusively by a user or the TCB and shall be logically isolated and unmistakably distinguishable from other paths."

Specific Application:

Systems at the B2-A1 levels are required to support a trusted path between users and the TCB. The requirement lists two examples (login and change of level) where this trusted path is required. It does not state what other situations, if any, require trusted path. Specifically, it does not state if trusted path is required for actions relating to Discretionary Access Control (DAC).

Possible Interpretations:

1. Trusted path is required for DAC actions.
2. Trusted path is not required for DAC actions.

Issues:

1. Does trusted path on DAC mechanisms have a useful purpose?
2. Can DAC information be set or modified in a secure manner without using trusted path?
3. Does this prevent Trojan Horse Attacks?

Rationale:

A user should have a way to determine or set DAC information in a secure manner. Any attack which attempts to manipulate DAC mechanisms directly should fail since the user would have to use a trusted path to validate the action. Unfortunately, this is not be enough to prevent a trojan horse from copying data it already has access to.

There are some side effects involved in adding trusted path to DAC. The effect on batch or background processing could be severe since someone is needed to validate the trusted path.

It may be possible to implement trusted path for DAC in a secure, useful and efficient way. However, it should not be required since it provides incomplete protection and may cause other problems. It should not be prohibited, either.

Accepted Interpretation:

Trusted path is not required for actions on DAC mechanisms.

Posted: 11 March 1987

FTLS Accuracy - Interpretation (Report No. C1-CI-01-87)

Criterion:

4.1.3.2.2 Design Specification and Verification (A1)

> "A formal top-level specification (FTLS) of the TCB shall be maintained that accurately describes the TCB in terms of exceptions, error messages, and effects. ... The FTLS shall be shown to be an accurate description of the TCB interface."

Possible Interpretations:

1. The FTLS may represent the TCB interface to each subject as an individual abstract machine; it should accurately describe all events affecting a single subject, but may ignore the effects of one subject on another when these would tend to make the specification more complex.
2. The FTLS should represent the TCB interface to all subjects executing on the machine in a unified way. Security-relevant effects of the actions of one subject that impinge on any other subject should always be accurately represented.

Specific Application:

Consider a system which allows a subject S to modify the access level of an object. This operation may well require the system to modify the current access permissions of other subjects. According to the first interpretation, the specification might not describe the modifications to the accesses of other subjects, or might describe only such modifications as subject S would be aware of. According to the second interpretation, the specification must describe the consequences of the operation on all subjects.

Issues:

1. An FTLS must support three main goals.
   (a) It must support a proof that the system design enforces the security policy, including the simple security and *-properties.
   (b) It must provide a basis for a catalogue of all covert storage channels.
   (c) It must provide a criterion of correctness for the implementation.

2. Interpretation 1 is unacceptable because it does not provide a basis for a proof that the system design enforces its security policy. The most that could be shown is that the subject invoking an action would never become aware of a breach of security caused by it (possibly indirectly). Similarly, there can be no assurance that an FTLS constructed according to interpretation 1 leads to a complete catalogue of covert channels, as flows of information to another process will not be indicated unless the first process can become aware of them. Finally, an FTLS based on interpretation 1 will not provide a criterion of correctness for the implementation. For instance, in the application mentioned above, the implementation would be insecure if it adhered to the description given in an FTLS based on interpretation 1.

3. The second interpretation leads to a more complex FTLS. Currently available tools for specification and verification have been stretched near their limits by the FTLSs to which they have been applied. Thus it is important to ensure that the increase in complexity will not overwhelm the available tools.

4. Uniform style is also an issue. If a specification departs at all from a literal description of the system as designed, it is important that the divergences are uniform, and that the reader can immediately recognize in which contexts he cannot expect literal description.

Accepted Interpretation:

The FTLS should accurately describe the operations that the TCB provides at its interface and the information that those operations return, dependent on the internal state of the TCB. The FTLS must also describe the effect of an operation on the internal state of the TCB, insofar as it can have security-relevant consequences for the behavior of future operations visible to any subject executing on the machine.

In particular, the FTLS must accurately specify all operations and the effects of those operations

a) on all system structures that it might have modified and that are visible to any user, and

b) on all structures associated with other subjects that can affect the error messages and return values that those subjects will subsequently receive.

By contrast, detail about the purely local information generated by an operation, such as the error messages it causes, may be omitted, so long as

c) any inaccuracies could only exaggerate the possible covert channels, but could never obscure actual covert channels;

d) a substantial simplification of the FTLS results; and

e) the simplifications are applied uniformly throughout the FTLS, and are clearly indicated in comments.

Posted: 11 March 1987

Rationale:

Point *a* ensures that the FTLS is a valid basis for a proof that the TCB will always be in a secure state. Point *b* ensures that the flow of information from one subject to another is accurately represented. Point *c* explicitly states that any inaccuracies in the FTLS will not prevent the analysis from providing a complete catalogue of all covert channels. Points *d* and *e* require that inaccuracies serve some genuine simplifying purpose, and that they should not prevent the FTLS from having a clear, uniform semantic style.

Audit - Interpretation (Report No. C1-CI-02-87)

Criterion:

3.3.2.2 - 4.1.2.2 Audit (B3-A1)

> "... The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded and, if the occurence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event."

Specific Application:

The Audit requirement contains several sub-sections to specify what may be called "real-time" action by the operating system in response to the occurrence of some security relevant events. These include: (1) a mechanism to monitor the occurrence or accumulation of the events, (2) the ability to recognize a violation of the security policy based on these events (such as invalid login attempts, and use of an audited covert channel), (3) immediate notification of the Security Administrator, (4) a threshold for such notification, (5) the ability to take action to terminate a security relevant event, (6) a threshold for this, and (7) terminating the event in a least disruptive mode. The real-time audit requirement must be dealt with as a whole to provide a uniform analysis of the intent.

The intent of the requirement is to provide a mechanism to recognize, report, and respond to a violation of the security policy more rapidly than required at the lower levels of the Criteria (usually by the Security Administrator reviewing an audit log at some time after the event).

Implications of this requirement may include: (1) a large extension to the audit mechanism from just posting security relevant events to significant amounts of data manipulation and analysis to discover any possible "imminent" violations of the security policy, (2) a definition of immediate notification, (3) the existence of two thresholds which may be settable by the Security Administrator, (4) autonomous action to terminate an event, and (5) a definition of least disruptive.

Possible Interpretations:

1. The requirement is to be taken literally. Significant amounts of analysis must be performed to recognize all possible imminent violations for any action or combinations of actions. Notification should be the

top priority of the TCB. Both bounds should be dynamically adjustable by the Security Administrator. The autonomous action by the system must be specific to the event and be the least disruptive of all possible actions.

2. Least disruptive is application dependent. No additional analysis beyond simple bounds checking by the auditing mechanisms need be done. Typical security relevant events which may lead to a violation of the security policy include: invalid login attempts and use of an audited covert channel. Notification of the Security Administrator should be as soon as practical. Both bounds should be settable. Any suitable autonomous action by the system which terminates the event is acceptable. Examples include: closing a covert channel, increasing the "noise" of a covert channel to decrease the effective bandwidth, not responding to a port which has had several bad logons, or terminating a user who attempts to repeatedly access a file to which they are denied access.

3. Least disruptive is application dependent. No additional analysis need be done. Notification should be in the normal order of events. Bounds may be set by the Security Administrator at system start-up. Any autonomous action by the system, such as halting the processor, is acceptable. Such a drastic reponse is allowed by interpretation C1-CI-01-83.

Accepted Interpretation:

1. The audit mechanism must provide bounds checking on counts and rates of events which may violate the security policy (e.g., invalid login attempts and the use of an audited covert channel).

2. Notification of the Security Administrator should be at the same priority as any other TCB message to an operator. It is desirable that this notification appear on a hardcopy device, non-scrolled video device, or an annunciator.

3. The bounds may be set by the Security Administrator at system start-up and, although it is not a requirement, it is preferable that they may be adjusted dynamically.

4. There is no requirement to demonstrate that an action is least disruptive of all possible actions. Any suitable autonomous action by the system which terminates the event is acceptable. Halting the system should be the last resort.

Posted: 11 May 1987

Rationale:

Least disruptive is application dependent. There is no requirement for extensive analysis based on past history or predictive projections beyond simple bounds checking of counts and rates. There is no requirement for extraordinary speed for notification. Notification should be at the same priority as any other TCB message to an operator. Bounds may be set at system start-up, but it is preferable that they may be set dynamically by the Security Administrator. The evaluation team is not required to do an exhaustive search of all possible mechanisms to determine if one is the least disruptive in any set of circumstances. The action should, however, be specific to the termination of the event. Halting the system should always be considered as an action of last resort.

Exportation of Labels-Interpretation (Report No. C1-CI-01-88)

Criterion:

3.1.1.3.2 Exportation of Labeled Information (B1)

> "... The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device."

Specific Application:

In B1 systems, device labels and label ranges for devices are not required. Therefore, the above seems to require that a system be able to audit a level change when a multi-level device such as a disk is changing level during its normal operations.

Possible Interpretations:

The following are possible interpretations of the above section of the Criteria:

1. The system should be able to audit any change of levels on any single or multi-level communications channel or I/O device attached to that system.

2. The system should be able to audit any change of levels for a single level communications channel or device.

Issues:

1. If auditing of security level changes on a multi-level device were to take place, the sheer volume of audit information generated would be both worthless and overwhelming. For instance, on a multi-level system, every time a disk was written to or read from by users at different levels, the write or read would have to be audited.

2. Useful information could be gleaned from audit data collected when a "single level" device changes levels. For instance, a tape drive is SECRET for user A, and then user B uses the tape drive next at UNCLASSIFIED. The change from S to U for the tape drive should be auditable.

Rationale:

Audit information generated as a result of paging or routine disk writes would be of little value to the auditor, because of its volume and granularity. Much more meaningful observations can be made by auditing changes from level to level on single level devices.

Accepted Interpretation:

Level changes on single level communication channels and I/O devices must be auditable. At B1, level changes on multi-level communication channels and I/O devices are not required to be auditable. Above B1, changes in device ranges must be auditable.

Posted: 21 April 1988

Audit Interpretation (Report No. C1-CI-01-89)

This interpretation has been superseded by "**I-0005** Action for audit log overflow."

Criterion:

2.2.2.2 - 4.1.2.2 Audit (C2-A1)

> "The TCB shall to able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects ..."

Specific Application:

This interp was prompted by the possibility of the audit data storage/collection media becoming full or otherwise inaccessible (e.g., device power loss or malfunction).

Possible Interpretations:

1. The audit trail must always be capable of completely and accurately reflecting all actions taken by users, provided that the actions had been specified as being auditable. Should a situation occur that causes the audit media to become full, or unavailable, the system must be capable of discontinuing processing of auditable events.
2. The audit trail must always be capable of completely and accurately reflecting all actions taken by users, provided that the actions had been specified as being auditable. Should a situation occur that causes the audit media to become full, or unavailable, the system need not be capable of discontinuing processing of auditable events.

Issues:

1. If the audit log overflows or otherwise becomes inaccessible the TCB is not maintaining an accurate audit trail (i.e., the data is being lost).
2. It may be more critical to an individual site that the system continue to run as opposed to keeping accurate audit data.

3. Some systems provide potential audit trails large enough to make their filling very unlikely under normal operation.

Rationale:

When an auditor/system administrator/security officer specifies the auditing of actions, the TCB should not violate that specification under any circumstances. The administrator, when specifying the auditing of that event, is implicitly stating that the site wishes to collect information on every occurrence of the specified action.

Some sites, however, may have a greater desire to continue to operate than to maintain an accurate and complete audit trail. These differing viewpoints suggest that a mechanism be capable of either continuing to operate or maintaining a completely accurate audit trail (or a combination of both).

Since the audit trail becoming full or inaccessible is a predictable system state, then a well defined solution is possible and can reasonably be expected.

Unless the auditing mechanism allows an authorized user to specify, in advance, what actions to take when an event occurs that may cause the audit media to become full or unavailable, it should be assumed that the site's wishes to maintain auditing data (and thus remain secure) are greater than its wishes to continue to operate.

Accepted Interpretation:

The TCB must maintain all audit data. If the audit data storage/ collection media should become full or otherwise inaccessible, the system must take well-defined action. When this condition arises, the system must give clear indication that the condition has occurred and it must also identify the action taken. By default, the action taken must be that the system cease performing auditable events (e.g., halt temporarily, shut down). The system may allow the administrator to explicitly specify an alternate action to be taken when the condition arises (e.g., discard some or all audit data, overwrite existing audit data, request new audit media). The issuance of this instruction must be auditable. The TFM must fully describe the administrator's options.

Posted: 9 January 1989

Audit Interpretation (Report No. C1-CI-02-89)

Criterion:

2.2.2.2 - 4.1.2.2 Audit (C2-A1)

> "The TCB shall to able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects ..."

Specific Application:

This interp was prompted by the possibility that under very extreme and infrequent conditions, some systems may lose small amounts of audit data. This loss may be attributed to a design tradeoff.

Possible Interpretations:

1. The audit mechanism must guarantee that the audit trail be capable of always completely and accurately reflecting all actions taken by users, provided that the actions had been specified as being auditable.

2. The audit trail must completely and accurately reflect most actions taken by users that have been specified to be recorded in the audit trail. The possible occurrence of situations that may cause audit records to not appear in, or to be discarded from, the audit trail shall be extremely rare (i.e., will almost never happen during normal system operation).

Issues:

1. It may be impossible to design an auditing mechanism which will never, under any circumstances, lose audit data.

2. It may be more critical to an individual site that the system continue to run as opposed to keeping accurate audit data.

3. In a B1-A1 system, it may be desirable to reduce trusted code by incurring an unlikely, but potential, loss of audit records.

Rationale:

When an auditor/system administrator/security officer specifies the auditing of actions, the TCB should not violate that specification under any circumstances. The administrator, when specifying the auditing of that event, is implicitly stating that the site wishes to collect information on every occurrence of the specified action.

While it is desirable to design an auditing mechanism that will never lose some amount of audit data, it is unreasonable to require that these situations can never occur. Some design tradeoffs may justify a situation in which small amounts of audit data may be unpredicatably lost. However, the number of these possible situations should be minimal and the odds of their occurring should be extremely small.

The audit mechanism should possess the ability to send warnings to system administrative personnel when events occur that indicate losses of audit data (e.g., X records lost).

Unless the auditing mechanism allows an authorized user to specify, in advance, what actions to take when an event occurs that may cause the loss of audit data, it should be assumed that the site's wishes to maintain auditing data (and thus remain secure) are greater than its wishes to continue to operate. Therefore, if an authorized user doesn't issue an explicit instruction specifying the action to be taken in the event of audit data loss, then the system must cease performing actions that would have been otherwise audited.

Accepted Interpretation:

The occurrence of events that may cause audit data to be unpredictably lost must be extremely rare (i.e., not under normal system load) and the number of records lost must be small (i.e., a few bytes as opposed to thousands of bytes). The TFM must completely identify the circumstances of potential audit data loss along with the possible quantity that may be lost. It must be extremely difficult for an untrusted process to cause the loss of audit data. Again, this possibility must be fully defined in the TFM.

The loss of any audit data should be clearly indicated and the action taken should be identified. In addition, the amount of audit data lost must be available. By default, the action taken must be for the system to cease performing events that would have been otherwise audited (e.g., halt temporarily, shut down). The system may allow the administrator to explicitly specify an alternate action to be taken when the condition arises (e.g., continue operating).

Posted: 9 January 1989

DAC Public Objects Interpretation (Report No. C1-CI-03-89)

Criterion:

2.2.1.1 C2 Discretionary Access Control

> "The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or both. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users."

Specific Application:

An operating system supports a set of objects that are accessible (read and/or execute access only) to all users of the system by definition (i.e., the system administrator can only remove the objects; he can not make them only available to any proper subset of the valid users of the system).

Possible Interpretations:

1. The system does not provide discretionary controls as required by the Criteria, and does not pass the DAC requirement.
2. Virtually all operating systems provide the concept of a "public" object, although such objects are not described nor mentioned in the Criteria. The evaluation community recognizes the utility of such mechanisms, and wishes to legitimize their existence with the following definition.

> A public object is an object for which the ADP system implementation permits all untrusted subjects to perform non-modifying operations (e.g. read, execute) on the object's contents and attributes, but permits only trusted subjects to modify the object's contents or attributes, and permits only trusted subjects to create or destroy such objects. Because the implementation always permits non-modify access by untrusted subjects, and therefore no access control decision is being made, such operations on public objects need not be auditable, but all other operations must be. In systems at B1 and above, public objects are implicitly labeled with the minimum label in the system, since all subjects are permitted to read them.

Rationale:

Virtually all computer systems support some form of public object, whether it be in the form of the system clock, a library of subroutines which is linked to each user's address space upon program execution, or a font library which may be prepended to a user's print job. There are scores of applications of public objects which are perfectly innocuous; that such objects were not explicitly legitimized in the TCSEC has not interfered with the fact of their existence.

Since no security threat is posed by the scenario related in interpretation 2), and the Criteria does not specifically disallow such a configuration, a mechanism which provides "public objects" should be allowed. Additionally, since a public object is by definition available for non-modify access to all users of the ADP system, the ability to audit the introduction of such an object into a user's address space provides no information of value to the system security administrator, and is therefore not required.

Accepted Interpretation:

Neither discretionary controls, nor auditability are required for public objects, as specified below:

> A public object is an object for which the ADP system implementation permits all untrusted subjects to perform non-modifying operations (e.g. read, execute) on the object's contents and attributes, but permits only trusted subjects to modify the object's contents or attributes, and permits only trusted subjects to create or destroy such objects. Because the implementation always permits non-modify access by untrusted subjects, and therefore no access control decision is being made, such operations on public objects need not be auditable, but all other operations must be. In systems at B1 and above, public objects are implicitly labeled with the minimum label in the system, since all subjects are permitted to read them.

Posted: 9 January 1989

Appendix B

Chronological Interpretation Summary

Date	Interpretation Number and Name	Classes
1993-10-20	**I-0002** - Delayed revocation of DAC access	C1,C2,B1,B2,B3,A1
1993-10-20	**I-0004** - Enforcement of audit settings consistent with protection goals	C2,B1,B2,B3,A1
1993-10-20	**I-0005** - Action for audit log overflow	C2,B1,B2,B3,A1
1993-10-20	**I-0006** - Audit of user-id for invalid login	C2,B1,B2,B3,A1
1993-10-20	**I-0007** - Assigning device level range	B2,B3,A1
1993-10-20	**I-0020** - DAC authority for assignment	C1,C2,B1,B2,B3,A1
1993-10-20	**I-0039** - Multilevel printers and page labeling	B1,B2,B3,A1
1993-10-20	**I-0040** - Requirements for overwrite label capability	B1,B2,B3,A1
1993-10-20	**I-0069** - Flexibility in packaging TFM	C1,C2,B1,B2,B3,A1
1993-10-20	**I-0073** - OK to audit decision regardless of whether action completed	C2,B1,B2,B3,A1
1993-10-20	**I-0193** - Standard system books as design documentation	C1,C2,B1,B2,B3,A1
1993-10-20	**I-0240** - Passwords may be used for card input	C1,C2,B1,B2,B3,A1
1993-10-20	**I-0244** - Flexibility in packaging SFUG	C1,C2,B1,B2,B3,A1
1993-10-20	**I-0275** - Single-level printers and page labeling	B1,B2,B3,A1
1994-04-18	**I-0096** - Blanking passwords	C1,C2,B1,B2,B3,A1
1994-04-18	**I-0170** - Functional tests required for object reuse	C2,B1,B2,B3,A1
1994-04-18	**I-0286** - Auditing unadvertised TCB interfaces	C2,B1,B2,B3,A1
1994-04-18	**I-0288** - Actions allowed before I&A	C1,C2,B1,B2,B3,A1
1994-04-19	**I-0001** - Delayed enforcement of authorization change	C1,C2,B1,B2,B3,A1
1994-04-19	**I-0022** - One set of banner pages around multiple outputs	B1,B2,B3,A1
1994-04-19	**I-0041** - Object reuse applies to all system resources	C2,B1,B2,B3,A1
1994-04-19	**I-0043** - Auditing use of unnamed pipe	C2,B1,B2,B3,A1
1994-04-19	**I-0172** - Audit of imminent security violations	B3,A1
1994-04-19	**I-0192** - Interface manuals as design documentation	C1,C2,B1,B2,B3,A1
1994-04-19	**I-0239** - Subject access revocation after change in user clearance	B1,B2,B3,A1
1994-04-19	**I-0285** - CM comparison source or object?	B2,B3,A1
1994-04-19	**I-0312** - Set-ID and the DAC requirement	C1,C2,B1,B2,B3,A1
1994-07-12	**I-0046** - Detailed audit record structure	C2,B1,B2,B3,A1
1994-07-12	**I-0084** - Audit least disruptive action	B3,A1
1994-11-16	**I-0003** - Access validation after object label change	B1,B2,B3,A1
1994-11-16	**I-0144** - Availability of diagnostics	C1,C2,B1,B2,B3,A1
1994-11-16	**I-0253** - Default page marking format	B1,B2,B3,A1
1994-12-05	**I-0222** - Passwords not acceptable for DAC	C1,C2,B1,B2,B3,A1
1994-12-05	**I-0254** - UNIX-style manual pages as DTLS	B2,B3,A1
1995-01-12	**I-0053** - Public objects and DAC	C1,C2,B1,B2,B3,A1
1995-01-12	**I-0213** - Administrator interface is part of TCB	C2,B1,B2,B3,A1
1995-01-12	**I-0315** - Restricted to trusted administrative interface	B3,A1

This page intentionally left blank

Appendix C

Interpretation Working Group Charter[1]

The Interpretations Working Group (IWG) has been created by the Trusted Product and Network Security Evaluations Division (C71) to improve on the current system of providing clarification of the requirements as stated in the Trusted Computer System Evaluation Criteria (TCSEC). The current system has the problems of:

- the interpretations being in a clumsy format,
- the interpretations not being available in a printed form,
- the official interpretations not being related to each other,
- the inability to produce needed interpretations in a timely manner, and
- inconsistency of team guidance when applied to essentially similar situations (i.e., "criteria creep").

The IWG's charter includes: identifying issues needing clarification; drafting proposed statements of clarification (which will be called interpretations); and, driving discussion on these statements to ensure closure. The IWG will also begin to build a body of "case law" by creating more system specific interpretations than currently done. Finally, the IWG will produce a suitable format for the periodic publication of completed interpretations.

The following is a description of the process governing the operation of the IWG. This process is also diagrammed in a chart that can be found on page 107 and this description is the supporting documentation for that chart. [Comments or suggested improvements on this description and/or the attached chart should be posted to the Criteria_Discussion forum.]

Input Sources

The IWG has identified five input sources through which issues can be raised to be addressed by the group. These input sources are:

- the Criteria_Discussion forum (public forum for discussion of TCSEC requirements and interpretations)
- the Interpretations forum (for internal use by evaluators to discuss TCSEC wording needing clarification)
- the Decisions forum (for internal use by evaluators to share decisions made with other evaluation teams)

[1] The contents of this appendix have been copied from transaction number 1588 of the Criteria_Discussion forum on Dockmaster.

- the TRB forum (for use by the TRB in their discussions on products being reviewed and for posting their recommendations to C71 management)
- Formal Interpretations

Additionally, the IWG will maintain an "IWG Issues List." This list will serve as a placeholder for issues that cannot be resolved on the first pass through the group due to a need for further analysis. These issues will be re-examined at a later date.

Each of the five identified input sources will be reviewed to compile the initial list of issues needing to be addressed. This can be considered the "IWG start-up phase." After the completion of this phase, the IWG will begin to monitor each input source for new issues as they are posted. This will constitute the normal operating procedure of the group for the identification of issues.

The current set of formal interpretations will be reviewed and appropriate interpretations of a new form will be developed. No new interpretations of the prior form will be produced.

Review and Approval Process

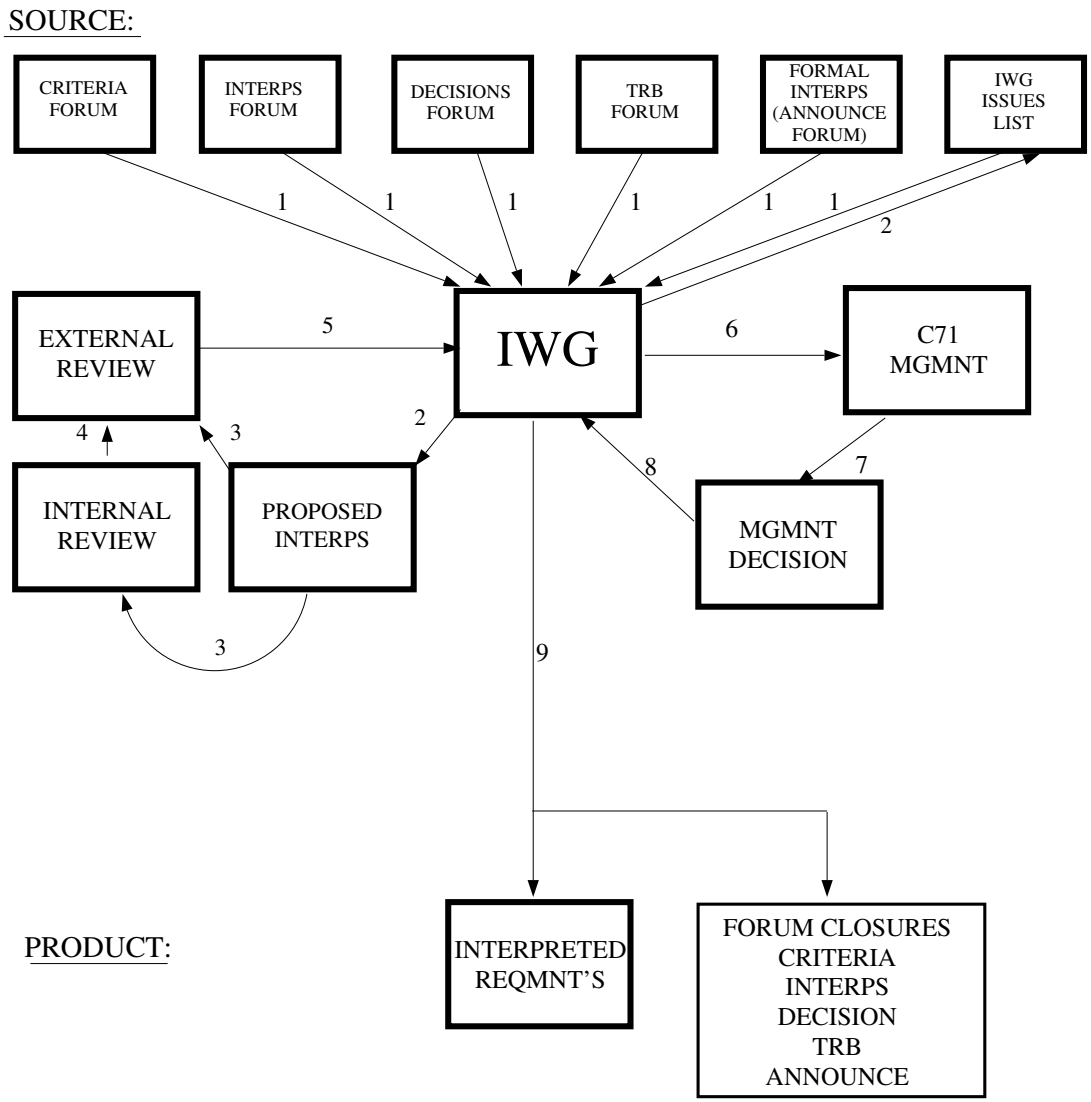
After issues are identified, they will be assigned to a member of the IWG for initial analysis. However, due to the large number of issues identified, it may be some time before the analysis on a specific issue begins. The scope and criticality of the issue will determine the order in which the issues will be addressed. The IWG member will research the issue to identify all relevant aspects and will propose a resolution of the issue to the group. When the group reaches consensus on an appropriate technical solution, the proposed interpretation will be posted to the Interpretations forum for internal evaluation community review and the Criteria_Discussion forum for external review. After a brief period of time (typically the length of time between IWG meetings, roughly 8 weeks), the IWG will incorporate appropriate comments into the proposed interpretation and, if completed, forward the interpretation to Trusted Product and Network Security Evaluations management for approval. Upon receiving management approval, the interpretation will be incorporated into the Interpreted TCSEC Requirements (to be periodically published) and to the appropriate forums (e.g., TRB, Criteria, Interpretations) to close discussions there.

At times, issues will be identified which cannot be resolved quickly. In these cases, the issue will be placed on the IWG Issues List and will be periodically checked to determine if a resolution may be attained.

Outputs

There are two types of output from the IWG. The first will be the closing statements on the appropriate forums ending the discussions of individual issues. These closing statements will include the statement of the interpretation. The second, and more important, is a document titled the Interpreted TCSEC Requirements. This document will be published periodically (initially after the first few interpretations are completed) and will contain interpretations for all issues resolved up to the time of publication. The form of this document will be a statement of each individual requirement, followed by all the interpretations that pertain to that requirement. Various indexes and cross references will also be included. In addition to the published document, an electronic version will be maintained on-line on Dockmaster.

IWG PROCESS



Legend: IWG - Interpretations Working Group
REQMNT'S - Requirements
MGMNT - Management

This page intentionally left blank

Appendix D
Acronyms

ACL ..... Access Control List

ADP ..... Automatic Data Processing

BSD ..... Berkeley Software Distribution

CI ..... Configuration Item

CMW ..... Compartmented Mode Workstation

CPU ..... Central Processing Unit

DAC ..... Discretionary Access Control

DAP ..... Design Analysis Phase

DBMS ..... Database Management System

DoD ..... Department of Defense

DOS ..... Disk Operating System

DTLS ..... Descriptive Top-Level Specification

EPL ..... Evaluated Products List

FER ..... Final Evaluation Report

FTLS ..... Formal Top-Level Specification

Gbyte ..... Gigabyte

I&A ..... Identification and Authentication

ID ..... Identifier

I/O ..... Input/Output

IPAR ..... Initial Product Assessment Report

IPC ..... Inter-Process Communication

IWG ..... Interpretations Working Group

Kbyte ..... Kilobyte

MAC ..... Mandatory Access Control

Mbyte ..... Megabyte

NCSC ..... National Computer Security Center

NSA ..... National Security Agency

PROM ..... Programmable Read-only Memory

PTR ..... Preliminary Technical Review

RAM ..... Random Access Memory

RAMP ..... Rating Maintenance Phase

RCO ..... Responsible Corporate Officer

RM-Plan .... Rating Maintenance Plan

ROM ..... Read-only Memory

SA ..... System Administrator

SFUG ..... Security Features User's Guide

TCB ..... Trusted Computing Base

TCSEC ..... *Trusted Computer System Evaluation Criteria*

TDI ..... *Trusted Database Management System Interpretation*

TNI ..... *Trusted Network Interpretation*

TFM ..... Trusted Facility Manual

TPOC ..... Technical Point of Contact

TRB ..... Technical Review Board

VAP ..... Vendor Assistance Phase

VM ..... Virtual Machine

VMM ..... Virtual Machine Monitor

VSA ..... Vendor Security Analyst

This page intentionally left blank

Appendix E
Bibliography and References

[1] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985.

[2] National Computer Security Center Trusted Database Management System Interpretation, NCSC-TG-021 Version 1, April 1991.

[3] National Computer Security Center Trusted Network Interpretation, NCSC-TG-005 Version 1, July 1987.