NCSC-TG-009
Library No. S230,512
Version 1

FOREWORD

This publication is issued by the National Computer Security Center (NCSC) as part of its program to promulgate technical computer security guidelines. This interpretation extends the Department of Defense Trusted Computer System Evaluation Criteria (DOD 5200.28-STD) to computer security subsystems.

This document will be used for a period of at least one year after date of signature. During this period the NCSC will gain experience using the Computer Security Subsystem Interpretation in several subsystem evaluations. After this trial period, necessary changes to the document will be made and a revised version issued.

Anyone wishing more information, or wishing to provide comments on the usefulness or correctness of the Computer Security Subsystem Interpretation may contact: Chief Technical Guidelines Division, National Computer Security Center, Fort George G. Meade, MD 20755-6000, ATTN: Cll.

PATRICK R GALLAGHER, JR. 16 September 1988
Director
National Computer Security Center

ACKNOWLEDGEMENT

Acknowledgment is extended to the members of the working group who produced this Interpretation. Members were: Michael W. Hale, National Computer Security Center (Chair); James P. Anderson; Terry Mayfield, Institute For Defense Analyses; Alfred W. Arsenault, NCSC; William Geer, NCSC; John C. Inglis, NCSC; Dennis Steinauer, National Bureau of Standards; Mario Tinto, NCSC; Grant Wagner, NCSC; and Chris Wilcox, NCSC.

Acknowledgement is further extended to those individuals who conducted thorough reviews and and provided constructive comments on this document. Reviewers included: Steve Lipner, Earl Boebert, Virgil Gligor, Debbie Downs, Len Brown, Doug Hardie, Steve Covington, Jill Sole and Bob Morris.

CONTENTS

LIST OF TABLES

1. INTRODUCTION

This document provides interpretations of the Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD or TCSEC) for computer security subsystems. A computer security subsystem (subsystem) is defined, herein, as hardware, firmware and/or software which can be added to a computer system to enhance the security of the overall system. A subsystem's primary utility is to increase the security of a computer system. The computer system that the subsystem is to protect is referred to as the protected system in this Interpretation.

When incorporated into a system environment, evaluated computer security subsystems may be very effective in reducing or eliminating certain types of vulnerabilities whenever entire evaluated systems are unavailable or impractical.

1.1 PURPOSE

This Interpretation has been prepared for the following purposes:

1. to establish a standard for manufacturers as to what security features and assurance levels to build into their new and planned computer security subsystem products to provide widely available products that satisfy trust requirements for sensitive applications;

2. to provide a metric to evaluate the degree of trust that can be placed in a subsystem for protecting classified and sensitive information;

3. to lend consistency to evaluations of these products by explicitly stating the implications that are in the TCSEC; and

4. to provide the security requirements for subsystems in acquisition specifications.

1.2 BACKGROUND

The Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD or TCSEC) was developed to establish uniform DoD policy and security requirements for "trusted, commercially available, automatic data processing (ADP) systems." Evaluation criteria defined in the TCSEC provides a standard to manufacturers as to what security features to build into their commercial products to satisfy trust requirements for sensitive applications, and serves as a metric with which to evaluate the degree of trust that can be placed in a computer system for the secure processing of classified or other sensitive information.

The TCSEC specifies a variety of features that a computer system must provide to constitute a complete security system. The security requirements specified in the TCSEC depend on and complement one another to provide the basis for effective implementation of a security policy in a trusted computer system. The effectiveness of any one security feature present within a system is, therefore, dependent to some degree on the presence and effectiveness of other security features found within the same system. Because it was intended to be used only for systems which incorporated all the security features of a particular evaluation class, the TCSEC does not, in all cases, completely specify these interdependencies among security features.

In addition to the class of trusted system products, there exists a recognized need for a class of computer security products which may not individually meet all of the security features and assurances of the TCSEC. Instead, these products may implement some subset of the features enumerated in the TCSEC and can potentially improve the security posture in existing systems. These products are collectively known as computer security subsystems.

Evaluation of computer security subsystems against a subset of the requirements given in the TCSEC has proven an extremely difficult task because of the implied dependencies among the various features discussed in the TCSEC. As a consequence, interpretations of these interdependencies and the relative merits of specific subsystem implementations have been highly subjective and given to considerable variation.

This document provides interpretations of the TCSEC for computer security subsystems in an effort to lend consistency to evaluations of these products by explicitly stating the implications in the TCSEC.

Evaluations can be divided into two types: (l) a product evaluation can be perforrned on a subsystem from a perspective that excludes the application environment, or (2) a certification evaluation can be done to assess whether appropriate security measures have been taken to permit an entire system to be used operationally in a specific environment. The product evaluation type is done by the National Computer Security Center (NCSC) through the Trusted Product Evaluation Process using this interpretation for subsystems. The certification type of evaluation lS done in support of a formal accreditation for a system to operate in a specific environment using the TCSEC.

1.3 SCOPE

This document interprets the security feature, assurance and documentation requirements of the TCSEC for subsystem evaluations. In this interpretation, the functional requirements of the TCSEC are divided into four general categories:

1. Discretionary Access Control (DAC)

2. Object Reuse (OR).

3. Identification and Authentication (I&A)

4. Audit (AUD)

These categories form the basis for classifying products to be evaluated as computer security subsystems.

The document, in addition to this introductory section, is organized into three major sections and a glossary. Section 2 contains the feature requirements for each of the above four categories on which subsystems evaluations are based. The requirements in this section are listed in increments, with only new or changed requirements being added for each subsequent class of the same feature. All requirements that are quoted from the TCSEC are in bold print for easy identification and are clarified, in the context of subsystems, by interpretation paragraphs.

Section 3 contains the assurance requirements for all subsystems. The assurances that are relevant to each category are listed here in the same format as the requirements in Section 2. Section 4 contains the requirements and interpretations for subsystem documentation, again, in the same fornat as Section 2.

The TCSEC-related feature and assurance requirements described herein are intended for the evaluation of computer security subsystems designed to protect sensitive information. This Interpretation, like the TCSEC, assumes that physical, administrative, and procedural protection measures adequate to protect the infornnation being handled are already in place.

This Interpretation can be used to support a certification evaluation. In fact, it would be helpful whenever subsystems are a part of the overall system being certified.

1.4 EVALUATION OF SUBSYSTEMS

1.4.1 Basis for Evaluation

Subsystems are evaluated for the specific security-relevant functions they perforrn. This Interpretation interprets the relevant TCSEC requirements for each function evaluated. So the function(s) for which subsystems are evaluated will be identified within its ratings. Each function has its own set of ratings as identified in Table 1.1. Subsystems that are evaluated for more than one function will receive a separate rating for each function evaluated.

TABLE 1.1. Possible Subsystem Ratings

SUBSYSTEM FUNCTION	POSSIBLE RATINGS
Discretionary Access Control	DAC/D DAC/Dl DAC/D2 DAC/D3
Object Reuse	OR/D OR/D2
Identification & Authentication	I&A/D I&A/Dl I&A/D2
Audit	AUD/D AUD/D2 AUD/D3

Although the requirements for subsystems are derived from the TCSEC, the ratings for subsystems will not directly reflect the TCSEC class they are derived from. Since subsystems, by their very nature, do not meet all of the requirements for a class Cl or higher computer system, it is most appropriate to associate subsystem ratings with the D division of the TCSEC. This Interpretation defines the Dl, D2 and D3 classes within the D division for subsystems. The Dl class is assigned to subsystems that meet the interpretations for requirements drawn from the Cl TCSEC class. Likewise, the D2 class consists of requirements and interpretations that are drawn from the C2 TCSEC class. The D3 subsystem class is reserved for DAC subsystems and audit subsystems that meet the B3 functionality requirements for those functions.

In addition to meeting the functionality requirements and interpretations, subsystems must also meet the assurance and documentation requirements in sections 3 and 4 of this document. The Dl and D2 classes have requirements and interpretations for assurances and documentation as well as functionality. The D3 class contains additional requirements and interpretations only for functionality, not for assurances or documentation. So, subsystems with this rating will adhere to the D2 assurance and documentation requirements and interpretations.

Like the classes within the TCSEC, the Dl, D2 and D3 classes are ordered hierarchically. Subsystems being evaluated for the Dl class must meet the requirements and interpretations for the Dl class. Subsystems being evaluated for the D2 class must meet the requirements and interpretations for the Dl class plus the additional requirements and interpretations for the D2 class. Subsystems being evaluated for the D3 class must meet the additional requirements and interpretations associated with the functionality at D3.

Although the subsystem requirements and interpretations are derived directly from the TCSEC, subsystems are not considered to be complete computer security solutions. There is no general algorithm to derive a system rating from an arbitrary collection of computer security subsystems. Any collection of individually evaluated subsystems must be evaluated as a whole to determine the rating of the resulting system. The ratings of the individual subsystems in a complete system are not a factor in the rating of that system.

1.4.2 Integration Requirements

Because all of the TCSEC requirements for a given rating class were intended to be implemented in a complete computer security system, many of the security features are dependent upon each other for support within the system. This poses a certain degree of difficulty with extracting only the relevant requirements from the TCSEC for a given feature. Further, this poses a fundamental problem for subsystems because there is an explicit dependency between security features that restricts the "independent" incorporation of subsystems into the system's environment. The problem has been handled in this Interpretation by discussing the integration requirements for each type of subsystem. The requirements for integration are discussed for each type of subsystem in a sub-section entitled, "Role Within Complete Security System." Furthermore, explicit requirements for integration are stated in the interpretations at appropriate points. The developer must show, and the evaluation shall validate, that the subsystem can be integrated into a system to fulfill its designated role.

Most all computer security subsystems will rely on other security-relevant functions in the envirومnent where they are implemented. Audit subsystems, for example, depend on an identification and authentication function to provide the unique user identities that are necessary for individual accountability. Also, it is important to realize that some of these functions may be dependent on each other in a cyclic fashion (e.g., I&A depends on DAC and DAC depends on I&A). In these cases, the cyclic dependencies should be removed either by complete integration of the functions or by modularizing the functions in a way that allows linear dependencies. Tl~is latter method is termed "sandwiching" and it requires the splitting of one function and surroundmg the other dependent function with the two functions resulting from the split. For example, in the case of DAC and I&A cyclic dependencies, one might split I&A into two parts so that there is a system I&A, a DAC subsystem, and a DAC module containing its own I&A functionality.

With the exception of object reuse, all functions implemented by subsystems will be dependent on other functions as shown in Table 1.2. The functions upon which any subsystem is dependent will be referred to as that subsystem's required supporting functions. These required supporting functions must be present in the subsystem's environment for the effective integration of the subsystem.

TABLE 1.2. Required Supporting Functions

SUBSYSTEM FUNCTION	REQUIRED SUPPORTING FUNCTIONS
~	
Discretionary Access Control	I&A Audit
Object Reuse	None
Identification & Authentication	Audit DAC2
Audit	I&A DAC2

Subsystems that are not self-sufficient in providing required supporting functions must, at a minimum, provide an interface to their required supporting functions. The

---

1 The audit supporting functions are required at D2.
2 Audit and/or authentication data must be protected through domain isolation or DAC.

evaluation team will perform tests to show whether the interface to the required supporting functions is reliable and works properly. The robustness of the required supporting functions on the other side of the interface will not be tested, as the scope of the subsystem evaluation is bounded by the interface.

A more integrated solution is for subsystems to be self- su~cient in providing all of their required supporting functions. Such subsystems w_ill be evaluated and assigned a separate rating for each function they provide. Unlike the previous solution, where only an interface is provided, each required supporting function is performed by the subsystem and must be a part of the subsystem evaluation.

1.4.3 WARNING

An overan system rating, such as that provided by the TCSEC, cannot be inferred from the application of one or more separately-rated subsystems. Mechanisms, interfaces, and the extent of required supporting functions for each subsystem may differ substantiany and may introduce significant vulnerabilities that are not present in systems where security features are designed with fun knowledge of interfaces and host system support. Therefore, incorporation of an evaluated subsystem into any system environment does not automaticany confer any rating to the resulting system.

2. FEATURE REQUIREMENTS

2.1 DISCRETIONARY ACCESS CONTROL (DAC) SUBSYSTEMS

2.1.1 Global Description of Subsystem Features

2.1.1.1 Purpose

This subsystem provides user-specified, controlled sharing of resources. This control is established from security policies which define, given identified subjects and objects, the set of rules that are used by the system to determine whether a given subject is authorized to gain access to a specific object.

DAC features include the means for restricting access to objects; the means for instantiating authorizations for objects; and the mechanisms for distribution, review, and revocation of access privileges, especially during object creation and deletion.

2.1.1.2 Role Within Complete Security System

The requirement is to give individual users the ability to restrict access to objects created or controlled by them. Thus, given identified subjects and objects, DAC includes the set of rules (group-oriented and/or individually-oriented) used by the subsystem to ensure that only specified users or groups of users may obtain access to data (e.g., based on a need-to-know).

A DAC subsystem controls access to resowces. As such, it shall be integrable with the operating system of the protected system and shall mediate all accesses to the protected resources. To fully protect itself and the resources it controls, the DAC subsystem must be interfaced to the protected system in such a way that it is tamperproof and always invoked.

DAC subsystems use the identifiers of both subjects and DAC-controlled objects as a basis for access control decisions. Thus, they must be supplied with the identifiers in a reliable manner. The DAC subsystem may supply subject identification for itself or it may rely on an I&A mechanism in the protected system or in another subsystem. It is also essential that DAC subsystems be implemented in an environment where the objects it protects are well defined and uniquely identified.

At the DAC/D2 class, the DAC subsystem must interface with an auditing mechanism. This auditing mechanism can be included within the DAC subsystem, or it may reside elsewhere in the subsystem's environment.

2.1.2 Evaluation of DAC Subsystems

Subsystems which are designed to implement discretionary access controls to assist a host in controlling the sharing of a collection of objects must comply with all of the TCSEC requirements as outlined below for features, assurances and documentation. Compliance with these requirements will assure that the subsystem can enforce a specifically defined group-oriented and/or individually-oriented discretionary access control policy.

As a part of the evaluation, the subsystem vendor shall set up the subsystem in a typical functional configuration for security testing. This will show that the subsystem interfaces correctly with the protected system to meet all of the feature requirements in this section and ali of the assurance and documentation requirements in Sections 3 and 4. It will also show that the subsystem can be integrated into a larger system environment.

The interpretations for applying the feature requirements to DAC subsystems are explained in the subsequent interpretations sections. The application of the assurances requirements and documentation requirements is explained in Sections 3 and 4, respectively.

2.1.3 Feature Requirements For DAC Subsystems

2.1.3.1 DAC/Dl

- TCSEC Quote:

"Cl: 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 special and control sharing of those objects by named indinduals or defined groups or both."

- Interpretation:

In the TCSEC quote, "TCB" is interpreted to mean "DAC subsystem".

2.1.3.1.1 Identified users and objects ~.

DAC subsystems must use some mechanism to determine whether users are authorized for each access attempted. At DAC/Dl, this mechanism must control access by groups of users. The mechanisms that can meet this requirement include, but are not limited to: access control lists, capabilities, descriptors, user profiles, and protection bits. The DAC mechanism uses the identification of subjects and objects to perform access control decisions. This implies that the DAC subsystem must interface with or provide some I&A mechanism. The evaluation shall show that user identities are available to DAC.

2.1.3.1.2 User-specified object sharing

The DAC subsystem must provide the capability for users to specify how other users or groups may access the objects they control. This requires that the user have a means to specify the set of authorizations (e.g., access control list) of all users or groups permitted to access an object and/or the set of all objects accessible to a user or group (e.g., capabilities).

2.1.3.1.3 Mediation

The checking of the specified authorizations of a user prior to granting access to an object is the essential function of DAC which must be provided. Mediation either allows or disallows the access.

2.1.3.2 DAC/D2

- TCSEC Quote:

"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 shan provide controls to limit propagation of access rights."

"C2: Add: The discretionary access control mechamsm shan, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls s~ll be capable of including or excluding access to the granularity of a single wer. Access permission to an object by users not already possessing access pernlission shan only be assigned by authorized users."

- Interpretation:

The following interpretations, in addition to the interpretations for the DAC/Dl Class, shall be satisfied at the DAC/D2 Class.

2.1.3.2.1 Single-user access granularity

The DAC/D2 class requires mdividual access controls; therefore, the granularity of user identification must enable the capabili~ to discern an individual user. That is, access control based upon group identi~ alone is insufflcient. To comply with the requirement, the DAC subsystem must either provide unique user identities through its own I&A mechanism or Mterface with an I&A mechanism that provides unique user identities. The DAC subsystem must be able to interface to an auditing mechanism that records data about access mediation events. The evaluation shall show that audit data is created and is available to the auditing mechanism.

2.1.3.2.2 Authorized user-specined object sharing

The ability to propagate access rights to objects must be lirnited to authorized users. This additional feature is incorporated to limit access rights propagation. This distribution of privileges encompasses granting, reviewing, and revoking of access. The ability to grant the right to grant propagation of access will itself be limited to authorized users.

2.1.3.2.3 Default protection

The DAC mechanism must deny all users access to objects when no explicit action has been taken by the authorized user to allow access.

2.1.3.3 DAC/D3

- TCSEC Quote:

"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: Furtherrnore, 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."

- Interpretation:

The following interpretation, in addition to the interpretations and requirements for the DAC/D2 class, shall be satisfied for the DACID3 class.

2.1.3.3.1 Access control lists for each object

The DAC subsystem shan anow users to specify the list of individuals or groups of individuals who can access each object. The list shan additionally specify the mode(s) of access that is anowed each user or group. This implies that access control lists associated with each object is the only acceptable mechanism to satisfy the DAC/D3 requirement.

2.1.4 Assurance Requirements for DAC Subsystems

DAC subsystems must comply with an of the assurance requirements for their given class as indicated below. The interpretations for these assurance requirements are contained in Section 3.

Subsystems at the DAC/Dl class must comply with:

- System Architecture (Dl)
- System Integrity (Dl)
- Security Testing (Dl)

Subsystems at the DAC/D2 and DAC/D3 classes must comply with:

- System Architecture (D2)
- System Integrity (D2)
- Security Testing (D2)

2.1.5 Documentation Requirements for DAC Subsystems

DAC subsystems must meet the documentation requirements listed below for their target rating class. The interpretations for these documentation requirements are contained in Section 4.

Subsystems at the DAC/Dl class must comply with:

- Security Features User's Guide (Dl)
- Trusted Facility Manual (Dl)
- Test Documentation (Dl)
- Design Documentation (Dl)

Subsystems at the DAC/D2 and DAC/D3 classes must comply with:

- Security Features User's Guide (D2)
- Trusted Facility Manual (D2)
- Test Documentation (D2)
- Design Documentation (D2)

2.2 OBJECT REUSE SUBSYSTEMS

2.2.1 Global Description of Subsystem Features

2.2.1.1 Purpose

Object reuse subsystems clear storage objects to prevent subjects from scavenging data from storage objects which have been previously used.

2.2.1.2 Role Within the Complete Security System

Object reuse can be used to prevent information scavenging by erasing information residue contained in previously used storage objects that have been released by the storage management system. Object reuse subsystems are most effective in environments where some security policy is implemented on the system.

To prevent scavenging of information from previously used storage objects, object reuse subsystems must be fully integrable with the operating system of the protected system. The object reuse subsystem must perform its function for all reusable storage objects on the protected system (i.e., main memory, disk storage, tape storage, I/O buffers, etc.).

Object reuse subsystems must be interfaced with the protected system in such a way that they are tamperproof and always invoked.

2.2.2 Evaluation of Object Reuse Subsystems

Subsystems which implement object reuse must comply with all of the TCSEC requirements as outlined below for features, assurances, and documentation. Compliance with these requirements will show that the subsystem can enforce object reuse adequately to receive an OR/D2 rating for object reuse.

As a part of the evaluation, the subsystem vendor shall set up the subsystem in a typical functional connguration for security testing. This will show that the subsystem interfaces correctly with the protected system to meet all of the feature requirements in this section and all of the assurance and documentation requirements in Sections 3 and 4. It will also show that the subsystem can be integrated into a larger system environment.

The interpretations for applying the feature requirements of object reuse subsystems are explained in the subsequent interpretations section. The application of the assurance requirements listed below is explained in Sections 3 and 4, respectively.

2.2.3 Feature Requirements for Object Reuse Subsystems

2.2.3.1 OR/D2

- TCSEC Quote:

"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."

- Interpretation:

In the TCSEC quote, "TCB" is interpreted to mean "protected system". Otherwise, this requirement applies as stated. The object reuse subsystem shall perform its function for all storage objects on the protected system that are accessible to users.

- Rationale/Discussion:

Object reuse subsystems must assure that no previously used storage objects (e.g., message buffers, page frames, disk sectors, magnetic tape, memory registers, etc.) can be used to scavenge residual information. Information remaining in previously used storage objects can be destroyed by overwriting it with meaningless or unintelligible bit patterns. An alternative way of approaching the problem is to deny read access to previously used storage objects until the user who has just acquired them has overwritten them with his own data.

Object reuse subsystems do not equate to systems used to eliminate magnetic remnance.

2.2.4 Assurance Requirements for Object Reuse Subsystems

Object reuse subsystems must comply with all of the assurance requirements shown below for the D2 class. The interpretations for these assurance requirements for Object Reuse subsystems are contained in Section 3.

- System Architecture (D2)
- System Integrity (D2)
- Security Testing (D2)

2.2.5 Documentation Requirements for Object Reuse Subsystems

Object reuse subsystems must meet the documentation requirements shown below for the D2 class. The interpretations for these documentation requirements are contained in Section 4.

- Security Features User's Guide (D2)
- Trusted Facility Manual (D2)
- Test Documentation (D2) ;
- Design Documentation (D2)

2.3 IDENTICATION & AUTHENTICATION (I&A) SUBSYSTEMS

2.3.1 Global Description of Subsystem Features

2.3.1.1 Purpose

This subsystem provides the authenticated identification of a user seeking to gain access to any resources under the control of the protected system.

2.3.1.2 Role Within Complete Security System

The I&A subsystem provides an authenticated user identification needed to provide accountability for and control access to the protected system. The granularity of user identification is determined by the requirements in this interpretation. The granularity increases from group identification at I&A/Dl to individual identification at I&A/D2.

The requirement is to be able to accurately authenticate the claimed identity of a user. The I&A subsystem must determine whether a user is authorized to use the protected system. For all authorized users, the I&A subsystem communicates the identity of the user to the protected system. This identity can then be used by the protected system or other subsystems to provide accountability for use of the system and access controls to protected objects on the system. To be effective and to protect the authentication data it uses, the I&A subsystem must be tamperproof and always invoked.

At I&A/D2, it is important that all uses of the I&A subsystem be recorded in an audit trail. The auditing of these actions may be performed entirely by the auditing mechanism on the I&A subsystem, or through an interface with an auditing mechanism in the protected system or another subsystem.

2.3.2 Evaluation of I&A Subsystems

Subsystems which are designed to implement I&A must comply with all of the TCSEC requirements outlined below for features, assurances, and documentation. Compliance with these requirements will assure that the subsystem can enforce, either wholly or in part, a specific I&A policy.

As a part of the evaluation, the subsystem vendor shall set up the subsystem in a typical functional configuration for security testing. This will show that the subsystem interfaces correctly with the protected system to meet all of the feature requirements in this section and all of the assurance and documentation requirements in Sections 3 and 4. It will also show that the subsystem can be integrated into a larger system environment.

The interetations for applying the feature requirements to I&A subsystems are explained in the subsequent interpretations sections. The application of the assurance requirements and documentation requirements listed in the next section is explained in Sections 3 and 4, respectively.

2.3.3 Feature Requirement for I&A Subsystems

2.3.3.1 I&A/Dl

- TCSEC Quote:

"Cl: 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."

- Interpretation:

The I&A subsystem shall require users to identify themselves to it before beginning to perforrn any other actions that the system is expected to mediate. Furthermore, the I&A subsystem shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The I&A subsystem shall protect authentication data so that it cannot be accessed by any unauthorized user.

The I&A subsystem shall, at a minimum, identify and authenticate system users. At I&A/Dl, users need not be individually identified.

- Rationale/Discussion:

Identification and Authentication must be based on at least a two-step process, which is derived from a combination of something the user possesses (e.g., smart card, magnetic stripe card), some physical attribute about the user (e.g., fingerprint, voiceprint), something the user knows (e.g., password, passphrase). The claimed identification of a user must be authenticated by an explicit action of the user. It is not acceptable for one step to be used as both identification and authentication. The claimed identity can be public. The measure used for authentication must be resistant to forging, guessing, and fabricating.

The I&A subsystem must interface to the protected system in such a way that it can reliably pass authenticated user identities to the protected system. The evaluation shall show that authenticated user identities can be passed to the protected system.

2.3.3.2 I&A/D2

- TCSEC Quote: -

"C2: Add: The TCB shan be able to enforce individual accountability by providing the capability to uniqueb identify each individual ADP system user. The TCB shall also ; provide the capabmty of associa~ ~is identity ~nth an auditable actiol~ taken by ; that indindual."

- Interpretation ~

The following interpretations, in addition to those interpretations for I&A/Dl, shall be satisfied at the I&A/D2 Class.

In the TCSEC quote, "TCB" is interpreted to mean "I&A subsystem." The I&A subsystem shall pass to the protected system a unique identifier for each individual.

The I&A subsystem shall be able to uniquely identify each individual user. This includes the ability to identify individual members within an authorized user group and the ability to identify specific system users such as operators, system administrators, etc.

The I&A subsystem shall provide for the audit logging of security-relevant I&A events. For I&A, the origin of the request (e.g., terminal ID, etc.), the date and time of the event, user ID (to the extent recorded), type of event, and the success or failure of the event shall be recorded. The I&A subsystem may meet this requirement either through its own auditing mechanism or by providing an interface for passing the necessary data to another auditing mechanism. ,

- Rationale/Discussion:

The intent of this requirement is for the I&A subsystem to supply a unique identity for each user to the protected system. The subsystem supplies a unique user identity which may or may not be used by an auditing mechanism. This auditing support is : required to maintain consistency with the C2 level of trust as defined by the TCSEC.

2.3.4 Assurance Requirements for I&A Subsystems

I&A subsystems must comply with all of the assurance requirements listed below for their given class. The interpretations for these assurance requirements to I&A subsystems are contained in Section 3.

Subsystems at the I&A/Dl class shall comply with:

- System Architecture (Dl)
- System Integrity (Dl)
- Security Testing (Dl) .

Subsystems at the I&A/D2 class shall comply with:

- System Architecture (D2)
- System Integrity (D2)
- Security Testing(D2)

2.3.5 Documentation Requirements for I&A Subsystems

I&A subsystems must meet the documentation requirements listed below for their target rating class. The interpretations for these documentation requirements are contained in Section 4.

Subsystems at the I&A/Dl class shall comply with:

- Security Features User's Guide (Dl)
- Trusted Facility Manual (Dl)
- Test Documentation (Dl)
- Design Documentation (Dl)

Subsystems at the I&A/D2 class shall comply with:

- Security Features User's Guide (D2)
- Trusted Facility Manual (D2)
- Test Documentation (D2)
- Design Documentation (D2)

2.4 AUDlT SUBSYSTEMS

2.4.1 Global Description of Subsystem Features

2.4.1.1 Purpose

Accountability is partly achieved through auditing. That is, data from security- relevant events is captured and passed to the audit mechanism to be recorded for use in detecting possible security breaches and providing a trace to the party responsible.

2.4.1.2 Role Within Complete Security System

The requirement is to be able to record security-relevant events in a manner that will allow detection and/or after-the-fact investigations to trace security violations to the responsible party.

An auditing subsystem must be capable of recording all security-relevant actions that take place throughout the computer system. To accomplish this goal, it must integrate itself into the mechanisms that mediate access and perform user identification and authentication, and capture data about the events they control. Additionally, an audit subsystem must be interfaced with the protected system in such a way that it is tamperproof and always invoked.

The auditing subsystem must be provided all of the necessary data associated with actions as specified in Section 2.4.3. The necessary data includes the unique identity of the user that is responsible for each action. This implies that an auditing subsystem must be augmented by an identification and authentication mechanism either within the subsystem itself or elsewhere on the system.

2.4.2 Evaluation of Auditing Subsystems

Subsystems which are designed to implement audit data collection and control functions for a host must comply with all of the TCSEC requirements as outlined below for features, assurances and documentatioi. Compliance with these features will assure that the subsystem, through its integration, can detect or generate the relevant audit data or can record all relevant audit data passed to it by the host or other subsystems.

As a part of the evaluation, the subsystem vendor shall set up the subsystem in a typical functional configuration for security testing. This will show that the subsystem interfaces correctly with the protected system to meet all of the feature requirements in this section and all of the assurance and documentation requirements in Sections 3 and 4. It will also show that the subsystem can be integrated into a larger system environrnent.

The interpretations for applying the feature requirements to auditing subsystems are explained in the subsequent interpretations sections. The application of the assurance requirements and documentation requirements is explained in Sections 3 and 4, respectively.

2.4.3 Feature Requirements For Auditing Subsystems

2.4.3.1 AUD/D2

- TCSEC Quote:

"C2: New: The TCB shan 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 shan 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, 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 identincation/authentication events the origin of request (e.g., terminal ID) shan 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. rne ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity."

- Interpretations:

The following subsections provide interpretations of the TCSEC requirements which shall be satisfied by auditing subsystems at AUD/D2.

~

2.4.3.1.1 Creation and management of audit trail

The auditing subsystem shall create and manage the audit trail of security-relevant " events in the system. If the other portions of the system are unable to capture data about such events, the auditing subsystem shall contain the necessary interfaces into the system to perform this function. Alternatively, the auditing subsystem might simply accept and store data about events if the other portions of the system are capable of creating such data and passing them on.

- Rationale/Discussion:

To meet this requirement, it is sufficient that the audit subsystem provides a set of calls which permit the system to supply the needed data as parameters that the audit subsystem puts into a data structure and routes to audit storage (or transmits securely to an audit logger).

2.4.3.1.2 Protection of audit data

It shall be demonstrated that the audit data is protected from unauthorized modification. This protection will be provided either by the subsystem itself or by its integration with the protected system.

- Rationale/Discussion:

The auditing subsystem might store the audit data in a dedicated data storage area that cannot be accessed by any subject on the system except the auditing subsystem itself and the system security officer (or system administrator through the auditing subsystem. Or, if the protected system has adequate access control facilities, the audit data might be stored on the protected system, using its access control mechanisms for protection.

2.4.3.1.3 Access control to audit

The audit mechanism, auditing parameters, and the audit data storage media shall be protected to ensure access is allowed only to authorized individuals. Individuals who are authorized to access the audit data shall be able to gain access only through the auditing subsystem.

- Rationale/Discussion:

This interpretation assumes that discretionary access controls or physical controls will be in place to keep unauthorized individuals from gaining access to the audit data.

2.4.3.1.4 Specific types of events
~
Data about all security relevant events must be recorded. The other portions of the system shall be able to pass data concerning these events to the auditing subsystem, or the auditing subsystem shall have the necessary code integrated into the other portions of the system to pass the data to the collection point.

2.4.3.1.5 Specific infolmation per event

All of the specific information enumerated in the TCSEC quote shall be captured for each recorded event. Of particular concern, is the recording of the user identity with each recorded event.

-Rationale/Discussion:

This implies that the audit subsystem must be able to acquire user identities from an I&A mechanism, which may be provided on the audit subsystem itself, on the protected system, or in a separate I&A subsystem. Whichever is the case, the evaluation shall show that the audit subsystem has a working interface to an I&A mechanism.

2.4.3.1.6 Ability to selectively audit individuals

The auditing subsystem shall have the ability to perform selection of audit data based on individual users.

- Rationale/Discussion:

This requirement can be satisfied by pre-selection of the information to be recorded in the audit log (selective logging) and/or by post-selection of information to be extracted from the audit log (selective reduction). The reduction of the audit log must be able to show all of the security-relevant actions performed by any specified individual. The intent of selective logging is to reduce the volume of audit data to be recorded by only recording audit data for those specific individuals that the systcm security officer (or system administrator) specifies. The intent of selective reduction is to reduce the large volume of audit data into a collection of intelligible information which can be more efficiently used by the system administrator.

2.4.3.2 AUD/D3

-TCSEC Quote:

"B3: Add: The TCB shal~ 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 securib relevant events continues, the system shall take the least disruptive action to terminate the event."

- Interpretation: The following interpretation, in addition to the interpretation and requirement for AUD/D2, shall be satisfied for the AUD/D3 class.

2.4.3.2.1 Real-time alarms

The auditing subsystem shall provide the capability for the security administrator to set thresholds for certain auditable events. Furthermore, when the thresholds are exceeded, the audit subsystem shall immediately notify the security administrator of an imminent security violation.

2.4.4 Assurance Requirements for Auditing Subsystems

Audit subsystems, whether being evaluated at AUD/D2 or AUD/D3, must comply with the assurance requirements listed below for the D2 class. The interpretations for these assurance requirements are contained in Section 3.

- System Architecture (D2)
- System Integrity (D2)
- Security Testing (D2)

2.4.5 Documentation Requirements for Auditing Subsystems "

Audit subsystems, whether being evaluated at AUD/D2 or AUD/D3, must meet the documentation requirements listed below for the D2 class. The interpretations for these documentation requirements are contained in Section 4.

- Security Features User's Guide (D2)
- Trusted Facility Manual (D2)
- Test Documentation (D2)
- Design Documentation (D2)

3. ASSURANCE REQUIREMENTS

Rated subsystems must provide correct and accurate operations. Assurance must be provided that correct implementation and operation of the subsystem's function exist throughout the subsystem's life cycle. The objective in applying these assurance requirements is to develop confidence that the subsystem has been implemented correctly and that it is protected from tampering and circumvention.

The requirement is that the subsystem must contain hardware/software mechanisms that can be independently evaluated through a combination of inspection and testing to provide sufficient assurance that the subsystem features enforce or support the functions for which the subsystem is intended. To receive a rating, a subsystem must meet the assurance requirements at the same level of trust as it has I met the requirements for functionality. The assurances must be applied to the different types of subsystems as described in the previous sections.

3.1 SUBSYSTEM ARCHITECTURE

Subsystem architecture evaluation is designed to provide operational assurances with regard to the design and implementation of the protection mechanisms of the subsystem and its interfaces to the host/host TCB.

3.1.1 Arch:D1

-TCSEC Quote:

"Cl: 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 controned by the TCB may be a defined subset of the subjects and objects in the ADP system."

- Interpretation:

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform. There are two specific elements of this requirement: Execution Domain Protection and Defined Subsets.

3.1.1.1 Execution Domain Protection

Protection of the subsystem's mechanism and data from external interference or tampering must be provided. The code and data of the subsystem may be protected' through physical protection (e.g., by the subsystem's dedicated hardware base) or by logical isolation (e.g., using the protected system's domain mechanism).

- Rationale and Discussion:

The subsystem may be contained entirely on its own hardware base which must protect the operational elements of the mechanisms. Alternatively, all or a portion of the subsystem may be implemented on the hardware of the host, in which case the host system's architecture must protect this portion from external interference or tampering.

3.1.1.2 Defined Subsets

I&A subsystems, when used for the system's I&A, define the subset of subjects under the control of the system's TCB.

DAC subsystems may protect a subset of the total collection of objects on the protected system.

3.1.2 Arch:D2

- TCSEC Quotes:

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

- Interpretation:

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

This requirement applies to all subsystems evaluated at the D2 class or the D3 class. The following interpretations explain how this requirement applies to specific functions performed by subsystems.

- Interpretation for DAC Subsystems:

All named objects which are in the defined subset of protected objects shall be isolated such that the DAC subsystem mediates all access to those objects.

- Interpretation for Auditing Subsystems:

The system's architecture shall ensure that the auditing mechanism cannot be bypassed by any subjects accessing those objects under the system's control.

-Interpretation for Object Reuse Subsystems

The notion of subsetting objects is not applicable to object reuse subsystems. Object reuse subsystems shall perform their function for all storage objects on the protected system that are accessible to users.

- Interpretation for I&A Subsystems:

This requirement applies to I&A subsystems. Authentication data shall be protected from unauthorized access. Access to the authentication data shall also be recorded in the audit trail.

3.2 SUBSYSTEM INTEGRITY

Subsystem integrity evaluation is designed to provide operational assurances with regard to the correct operation of the protection mechanisms of the subsystem and its interfaces to the protected system.

3.2.1 Integity:D1

-TCSEC Quote

"Cl: New: Hardware and/or software features shan be provided that can be used to periodicany ~aUdate the correct operation of the on site hardware and firmware elements of the TCB."

- Interpretation:

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

This requirement applies to an subsystems evaluated at any class, regardless of the functions they perform.

- Rationale/Discussion

The capability must exist to validate the correct operation of all hardware and firrnware elements of the system regardless of whether they reside within the subsystem, the protected system, or other interfacing subsystems. If the hardware and/or firmware elements of the protected system or other interfacing subsystems play an integral role in the protection and/or correct operation of the subsystem, then they must comply with this requirement as though they were part of the subsystem.

3.2.2 Integrity:D2

There are no additional requirements for System Integrity at D2.

3.3 SECURITY TESTING

Testing, as part of the evaluation, is designed to provide life cycle assurances with regard to the integrity of the subsystem. Further, testing provides additional assurances regarding the correct operation of the protection mechanisms of the subsystem and the subsystem's interfaces to the protected system. These mechanisms and their interfaces to the protected system, are termed the Subsystem's Security- Relevant Portion (SRP).

3.3.1 Test:Dl

- TCSEC Quote:

"Cl: New: The securib mechanisms of the ADP system shan be tested and found to work as claimed in the system documentation. Testing shan be done to assure that there are no ob~ious ways for an unauthorized wer to bypass or otherwise defeat the security protection mechanisms of the TCB. (See the Security Testing Guidelines.) "

- Interpretation

This requirement applies to all subsystems evaluated at any class, regardless of the function(s) they perform. In the TCSEC quote, "TCB" is interpreted to mean subsystem.

The subsystem's SRP shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected system shall not cause obvious flaws to the resulting system. _

Test results shall show that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the subsystem's SRP.

- Rational/Discussion:

Security testing is a very important part of subsystem evaluations. It is essential that the subsystem be demonstrated to operate securely.

3.3.2 Test:D2

- TCSEC Quote:

"C2: Add: Testing shan also include a search for obvious flaws that would anow nolation of resource isolation, or that would permit unauthorized access to the audit or authentication data."

- Interpretation:

This requirement applies to the testing of the SRP of any subsystem evaluated at the D2 class or the D3 class.

- Rationale/Discussion

The requirement as written in the TCSEC quote is directly applicable. This requirement is to ensure that subsystems at D2 cannot be circumvented or tampered with.

4. DOCUMENTATION REQUIREMENTS

Documentation shan produce evidence that the subsystem can and does provide specified security features. The evaluation will focus on the completeness of this evidence through inspection of documentation structure and content and through a mapping of the documentation to the subsystem's implementation and its operation.

4.1 SECURITY FEATURES USER'S GUIDE

4.1.1 SFUG:Dl

- TCSEC Quote:

"Cl: New: A single summaIy, 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."

- Interpretation:

All subsystems shall meet this requirement in that they shall describe the protection mechanisms provided by the subsystem.

- Rationale/Discussion:

It is recognized that some subsystems may be partially or completely transparent to the general user. In such cases, this requirement can be met by documenting the functions the subsystem performs so users will be aware of what the subsystem does. Other subsystems which have a very limited user interface may not need to be accompanied by more than a pocketsize card available to every user. In short, the documentation required to meet this requirement need not be elaborate, but must be clear and comprehenslve.

4.1.2 SFUG:D2

-Interpretation:

There are no additional requirements at the D2 class.

4.2 TRUSTED FACILITY MANUAL

4.2.1 TFM:Dl

- TCSEC Quote :

"Cl: New: A manual addressed to the ADP system admmistrator shan present cautions about functions and prvileges that should be controlled when running a secure facility."

- Interpretation:

This requirement applies to all subsystems in that the manual shall present cautions about functions and privileges provided by the subsystem. Further, this manual shall present specific and precise direction for effectively integrating the subsystem into the overall system.

4.2.2 TFM:D2

- TCSEC Quote:

"C2: Add: The procedures for examining and maintaMing the audit files as well as the detailed audit record structure for each type of audit event shall be given."

- Interpretation:

This requirement applies directly to all auditing subsystems and to other subsystems that maintain their own audit data concerning events that happen under their control. For subsystems that create audit data and pass it to an external auditing collection and maintenance facility, the audit record structure shall be documented; however, the procedures for examination and maintenance of audit files may be left to the external auditing facility.

4.3 TEST DOCUMENTATION

4.3.1 TD:Dl

- TCSEC Quote:

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

- Interpretation:

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the subsystem being tested, the protected system, and other subsystems shall be described.

4.3.2 TD:D2

-Interpretation

There are no additional requirements at the D2 class.

4.4 DESIGN DOCUMENTATION

4.4.1 DD:Dl

- TCSEC Quote:

"Cl: 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. "

- Interpretation:

This requirement applies directly to all subsystems. Specifically, the design documentation shall state what types of threats the subsystem is designed to protect against (e.g., casual browsing, determined attacks, accidents). This documentation shan show how the protection philosophy is translated into the subsystem's SRP. Design documentation shan also specify how the subsystem is to interact with the protected system and other subsystems to provide a complete computer security system. If the SRP is modularized, the interfaces between these modules shall be described.

4.4.2 DD:D2

There are no additional requirements for Design Documentation at the D2 class.

5- GLOSSARY

Accreditation - The offlcial authorization that is granted to an ADP system to process sensitive information in its operational environment, based upon , comprehensive security evaluation of the system's hardware, firmware, and software . security design, configuration and implementation of the other system procedural, administrative, physical, TEMPEST, personnel, and comrnunications controls.

Audit - The procedure of capturing, storing, maintaining, and managing data concerning security-relevant events that occur on a computer system. The data recorded are intended for use in detecting security violations and tracing thosc violations to the responsible individual.

Audit trail - A set of records that collectively provide documentary evidence of processing users to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.

Authenticate - To establish the validity of a claimed identity.

Authorization - Permission which establishes right to access information.

Certification evaluation - The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes " the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

Computer security subsystem - Hardware, firmware and/or software which are added to a computer system to enhance the security of the overall system.

Group user - A user of a computer system whose system identification is the name of a defined group of users on that system.

Individual user - A user of a computer system whose system identification is unique, in that no other user on that system has that same identification.

Named object - An object which is directly manipulable at the TCB interface. Thc object must have meaning to more than one process.

Product evaluation - Thc technical evaluation of a product's security features to determine the level of trust that can be placed in that product as defined by thc NCSC. evaluation criteria for that type of product (e.g., operating system, database management system, computer network, computer security subsystem). Product evaluations do not consider the application of the product in the evaluation.

Protected system - The system being protected. In the context of computer security subsystems, a stand-alone computer system or a computer network to which a subsystem is attached to pronde some computer security function.

Security Relevant Portion (SRP) - The protection-critical mechanism of the subsystem, the subsystem's interface(s) to the protected system, and interfaces to the mechanisms providing required supporting functions. For most cases, the SRP encompasses the entire subsystem.

Subsystem - See "computer security subsystem."

System - The combination of the protected system and the computer security subsystem.

*U.S. GOVERNMENT PRINTING OFFICE: 1989-225-703