CSC-STD-003-85

COMPUTER SECURITY REQUIREMENTS

GUIDANCE FOR APPLYING THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA IN SPECIFIC ENVIRONMENTS

25 June 1985

CSC-STD-003-85
Library No. S-226,727

FOREWORD

This publication, Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, is being issued by the DoD Computer Security Center (DoDCSC) under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." It provides guidance for specifying computer security requirements for the Department of Defense (DoD) by identifying the minimum class of system required for a given risk index. System classes are those defined by CSC-STD-001-83, Department of Defense Trusted Computer System Evaluation Criteria, 15 August 1983. Risk index is defined as the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by the system. This guidance is intended to be used in establishing minimum computer security requirements for the processing and/or storage and retrieval of sensitive or classified information by the Department of Defense whenever automatic data processing systems are employed. Point of contact concerning this publication is the Office of Standards and Products, Attention: Chief, Computer Security Standards.

25 June 1985

Robert L. Brotzman
Director
DoD Computer Security Center

ACKNOWLEDGMENTS

Acknowledgment is given to the following for formulating the computer security requirements and the supporting technical and procedural rationale behind these requirements: Col Roger R. Schell, formerly DoDCSC, George F. Jelen, formerly DoDCSC, Daniel J. Edwards, Sheila L. Brand, and Stephen F. Barnett, DoDCSC.

Acknowledgment is also given to the following for giving generously of their time and expertise in the review and critique of these computer security requirements: CDR Robert Emery, OJCS, Dan Mechelke, 902nd MI Gp, Mary Taylor, DAMI-CIC, Maj. Freeman, DAMI-CIC, Ralph Neeper, DAMI-CIC, Duane Fagg, NAVDAC, H. O. Lubbes, HAVE LEX, Sue Berg, OPNAV, Susan Tominack, NAVDAC, Lt. Linda Fischer, OPNAV, Eugene Epperly, ODUSD(P), Maj. Grace Culver, USAF- SITT, Capt Mike Weidner, ASPO, and James P. Anderson, James P. Anderson & Co.

And finally, special recognition is extended to H. William Neugent and Ingrid M. Olson of the MITRE Corporation and to Alfred W. Arsenault of the DoDCSC for preparation of this document.

TABLE OF CONTENTS

LIST OF TABLES

1.0 INTRODUCTION

This document establishes computer security requirements for the Department of Defense (DoD) by identifying the minimum class of system required for a given risk index. The classes are those defined by CSC-STD-001-83, Department of Defense Trusted Computer System Evaluation Criteria (henceforth referred to as the Criteria).(1) A system's risk index is defined as the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by the system. [1]

The recommendations in this document are those that the DoD Computer Security Center (DoDCSC) believes to be the minimum adequate to provide an acceptable level of security. These recommendations are made in part due to the fact that there is no comprehensive policy in effect today which covers this area of computer security. Where current policy does exist, however, this document shall not be taken to supersede or override that policy, nor shall it be taken to provide exemption from any policy covering areas of security not addressed in this document.

Section 2 of this document provides definitions of terms used. Risk index computation is described in Section 3, while Section 4 presents the computer security requirements.

---

[1] Since a clearance implicitly encompasses lower clearance levels (e.g., a Secret- cleared user has an implicit Confidential clearance), the phrase "minimum clearance of the system users" is more accurately stated as "maximum clearance of the least cleared system user." For simplicity, this document uses the former phrase.

2.0 DEFINITIONS

Application

Those portions of a system, including portions of the operating system, that are not responsible for enforcing the system's security policy.

Category

A grouping of classified or unclassified but sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have appropriate authorization (e.g., proprietary information (PROPIN), information that is Not Releasable to Foreign Nationals (NOFORN), compartmented information, information revealing sensitive intelligence sources and methods (WNINTEL)). Closed security environment

An environment in which both of the following conditions hold true:

1. Application developers (including maintainers) have sufficient clearances and authorizations to provide acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of the data to be processed is Confidential or less, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of the data to be processed is Secret or above, developers have at least a Secret clearance.

2. Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications.

Compartmented security mode

The mode of operation which allows the system to process two or more types of compartmented information (information requiring a special authorization)6565 or any one type of compartmented information with other than compartmented information. In this mode, all system users need not be cleared for all types of compartmented information processed, but must be fully cleared for at least. Top Secret information for unescorted access to the computer.

Configuration control

Management of changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system.

Controlled security mode

The mode of operation that is a type of multilevel security mode in which a more limited amount of trust is placed in the hardware/software requirement base of the system, with resultant restrictions on the classification levels and clearance levels that may be supported.

Dedicated security mode

The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

Environment

The aggregate of external circumstances, conditions, and events that affect the development, operation, and maintenance of a system.

Malicious logic

Hardware, software, or firmware that is intentionally included in a system for the purpose of causing loss or harm (e.g., Trojan horses).

Multilevel security mode

The mode of operation which allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present.

Open security environment

An environment in which either of the following conditions holds true:

1. Application developers (including maintainers) do not have sufficient clearance (or authorization) to provide an acceptable presumption that they have not introduced malicious logic. (See "Closed security environment" for definition of sufficient clearance.)

2. Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications.

Risk index

The disparity between the minimum clearance or authorization of system users and the maximum sensitivity (e.g., classification and categories) of data processed by a system.

Sensitive information

Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

System

An assembly of computer hardware, software, and firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

System high security mode

The mode of operation in which system hardware/software is only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed.

System users

Those individuals with direct connections to the system, and also those individuals without direct connections who receive output or generate input that is not reliably reviewed for classification by a responsible individual. The clearance of system users is used in the calculation of risk index.

For additional definitions, refer to the Glossary of TheCriteria.(1)

3.0 RISK INDEX COMPUTATION

The initial step in determining the minimum evaluation class required for a system is to determine the system's risk index. The risk index for a system depends on the rating associated with the system's minimum user clearance (Rmin) taken from Table 1 and the rating associated with the system's maximum data sensitivity (Rmax) taken from Table 2. The risk index is computed as follows:

Case a. If Rmin is less than Rmax, then the risk index is determined by subtracting Rmin from Rmax. [1]

Risk Index = Rmax - Rmin

Case b. If Rmin is greater than or equal to Rmax, then

```
            !---1, if there are categories on the system to which some users
            !      are not authorized access
            !
Risk Index =!
            !
            !--- 0, otherwise
```

[1] There is one anomalous value that results because there are two "types" of Top Secret clearance and only one "type" of Top Secret data. When the minimum user clearance is TS/BI and the maximum data sensitivity is Top Secret without categories, then the risk index is 0 (rather than the value 1- which would result from a straight application of the formula)

TABLE 1

RATING SCALE FOR MINIMUM USER CLEARANCE [1].

	RATING (R_{min})
Uncleared (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret	3
Top Secret (TS)/Current Background Investigation (BI)	4
Top Secret (TS)/current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

---

[1] The following clearances are as defined in DIS Manual 20-1(2): Confidential, Secret, Top Secret/Current Background Investigation, Top Secret/Current Special Background Investigation.

TABLE 2

RATING SCALE FOR MAXIMUM DATA SENSITIVITY

MAXIMUM DATA SENSITIVITY RATINGS [2] WITHOUT CATEGORIES (Rmax)	RATING (Rmax)	MAXIMUM DATA SENSITIVITY WITH CATEGORIES [1]	
Unclassified(U)	0	Not Applicable [3]	
Not Classified but Sensitives [4]	1	N With One or More Categories	2
Confidential(C)	2	C With One or More Categories	3
Secret (S)	3	S With One or More Categories With No More Than One Category Containing Secret Data	4
		S With Two or More Categories Containing Secret Data	5
Top Secret (TS)	5 [5]	TS With One or More Categories With No More Than One Category Containing Secret or Top Secret Data	6
		TS With Two or More Categories Containing Secret or Top Secret Data	7

----

[1] The only categories of concern are those for which some users are not authorized access. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level.

[2] Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.

[3] Since categories are sensitive and unclassified data is not, unclassified data by definition cannot contain categories.

[4] Examples of N data include financial, proprietary, privacy, and mission sensitive data. In some situations (e.g., those involving extremely large financial sums or critical mission sensitive data), a higher rating may be warranted. The table prescribes minimum ratings.

[5] The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This

difference derives from the fact that the loss of Top Secret data causes exceptionally grave damage to the national security, whereas the loss of Secret data causes only serious damage.

4.0 COMPUTER SECURITY REQUIREMENTS

Table 3 identifies the minimum evaluation class appropriate for systems based on the risk index computed in Section 3. The classes identified are those from The Criteria.(1) A risk index of 0 encompasses those systems operating in either system high or dedicated security mode. Risk indices of 1 through 7 encompass those systems operating in multilevel, controlled, compartmented, or the Navy's limited access security mode; that is, those systems in which not all users are fully cleared or authorized access to all sensitive or classified data being processed and/or stored in the system. In situations where the local environment indicates that additional risk factors are present, a system of a higher evaluation class may be required.

TABLE 3

COMPUTER SECURITY REQUIREMENTS

RISK INDEX	SECURITY OPERATING MODE	MINIMUM CRITERIA CLASS FOR OPEN ENVIRONMENTS [4]	MINIMUM CRITERIA CLASS FOR CLOSED ENVIRONMENTS [4]
0	Dedicated	No Prescribed Minimum [1]	No Prescribed Minimum [1]
0	System High	C2[2]	C2[2]
1	Limited Access, Controlled, Compartmented, Multilevel	B1[3]	B1[3]
2	Limited Access, Controlled, Compartmented, Multilevel	B2	B2
3	Controlled, Multilevel	B3	B2
4	Multilevel	A1	B3
5	Multilevel	*	*
6	Multilevel	*	*
7	Multilevel	*	*

----

[1] Although there is no prescribed minimum class, the integrity and denial of service requirements of many systems warrant at least class C1 protection.

[2] If the system processes sensitive or classified data, at least a class C2 system is required. If the system does not process sensitive or classified data, a class C1 system is sufficient.

[3] Where a system processes classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being processed, at least a class B2 system is required.

[4] The asterisk (*) indicates that computer protection for environments with that risk index is considered to be beyond the state of current computer security technology. Such environments must augment technical protection with physical, personnel, and/or administrative security solutions.

REFERENCES

1. DoD Computer Security Center, DoD Trusted Computer System Evaluation Criteria, CSC-STD-001-83, 15 August 1983.

2. Defense Investigative Service (DIS) Manual 20-1, Manual for Personnel Investigations, 30 January 1981 .