TECHNICAL RATIONAL BEHIND 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-004-85
Library No. S-226,728

FOREWORD

This publication, Technical Rationale Behind CSC-STD-003-85: 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." This document presents background discussion and rationale for CSC-STD-003-85, Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments. The computer security requirements identify 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 an-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

Special recognition is extended to H. William Neugent and Ingrid M. Olson of the MITRE Corporation for performing in-depth analysis of DoD policies and procedures and for preparation of this document.

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 this document: CDR Robert Emery, OJCS, Dan Mechelke, 902nd Ml Gp, Mary Taylor, DAMI-CIC, Maj. Freeman, DAMI- CIC, Ralph Neeper, DAMI-CIC, Duane Fagg, NAVDAC, H. O. Lubbes, NAVELEX, Sue Berg, OPNAV, Susan Tominack, NAVDAC, Lt Linda Fischer, OPNAV, Eugene Epperly, ODUSD(P), Maj Grace Culver, USAF-SITT, Capt Mike Weidner, ASPO, Alfred W. Arsenault, DoDCSC, James P. Anderson, James P. Anderson & Co., and Dr. John Vasak, MITRE Corporation.

TABLE OF CONTENTS

LIST OF TABLES

1.0 INTRODUCTION

The purpose of this technical report is to present background discussion and rationale for Computer Security Requirements--Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments(1) (henceforth referred to as the Computer Security Requirements). The requirements were prepared in compliance with responsibilities assigned to the Department of Defense (DoD) Computer Security Center (DoDCSC) under DoD Directive 5215.1, which tasks the DoDCSC to "establish and maintain technical standards and criteria for the evaluation of trusted computer systems."(2)

DoD computer systems have stringent requirements for security. In the past, these requirements have been satisfied primarily through physical, personnel, and information security safeguards.(3) Recent advances in technology make it possible to place increasing trust in the computer system itself, thereby increasing security effectiveness and efficiency. In turn, the need has arisen for guidance on how this new technology should be used. There are two facets to this required guidance:

a. Establishment of a metric for categorizing systems according to the security protection they provide.

b. Identification of the minimum security protection required in different environments.

The DoD Trusted Computer System Evaluation Criteria (henceforth referred to as the Criteria), developed by the DoDCSC, satisfy the first of these two requirements by categorizing computer systems into hierarchical security classes.(4) The Computer Security Requirements satisfy the second requirement by identifying the minimum classes appropriate for systems in different risk environments. They are to be used by system managers in applying the Criteria and thereby in selecting and specifying systems that have sufficient security protection for specific operational environments.

Section 2 of this document discusses the risk index. Section 3 presents a discussion of the Computer Security Requirements for open security environments. Section 4 presents a discussion of the Computer Security Requirements for closed security environments. A summary of the Criteria is contained in Appendix A. Appendix B contains a detailed description of clearances and data sensitivities, and Appendix C describes the environmental types. A glossary provides definitions of many of the terms used in this document.

1.1 Scope and Applicability

This section describes the scope and applicability for both this report and the Computer Security Requirements. The primary focus of both documents is on the technical aspects (e.g., hardware, software, configuration control) of computer security, although the two documents also address the relationship between computer security and physical, personnel, and information security. While communications and emanations security are important elements of system security, they are outside the scope of the two documents.

Both documents apply to DoD computer systems that are entrusted with the protection of information, regardless of whether or not that information is classified, sensitive, national security-related, or any combination thereof. Furthermore, both documents can be applied throughout the DoD.(5,6,7,8,9)

The two documents are concerned with protection against both disclosure and integrity violations. Integrity violations are of particular concern for sensitive unclassified information (e.g., financial data) as well as for some classified applications (e.g., missile guidance data).

The recommendations of both this report and the Computer Security Requirements are stated in terms of classes from the Criteria. Embodied in each class and therefore encompassed within the scope of both documents are two types of requirements: assurance and feature requirements. Assurance requirements are those that contribute to confidence that the required features are present and that the system is functioning as intended. Examples of assurance requirements include modular design, penetration testing, formal verification, and trusted configuration management. Feature requirements encompass capabilities such as labeling, authentication, and auditing.

1.2 Security Operating Modes

DoD computer security policy identifies several security operating modes, for which the following definitions are adapted:(10,11,12,13)

a. 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 fulltime operation or for a specified period of time.

b. 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, and 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.

c. 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.

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

e. 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) or any one type of compartmented information with other than compartmented information. In this mode, system access is secured to at least the Top Secret (TS) level, but all system users need not necessarily be formally authorized access to all types of compartmented information being processed and/or stored in the system.

In addition to these security operating modes, Service policies may define other modes of operation. For example, Office of the Chief of Naval Operations (OPNAV) Instruction 5239. IA defines Limited Access Mode for those systems in which the minimum user clearance is uncleared and the maximum data sensitivity is not classified but sensitive (6)

2.0 RISK INDEX

The evaluation class appropriate for a system is dependent on the level of security risk inherent to that system. This inherent risk is referred to as that systems risk index. Risk index is defined as follows:

> The disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by a system.

The Computer Security Requirements are based upon this risk index. Although there are other factors that can influence security risk, such as mission criticality, required denial of service protection, and threat severity, only the risk index is used to determine the minimum class of trusted systems to be employed, since it can be uniformly applied in the determination of security risk. The risk index for a system depends on the rating associated with the system's mimimum 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.2

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 (i.e., if there are no categories on the system or if all users are authorized access to all categories)

> Example: For a system with a minimum user clearance of Confidential and maximum data sensitititivy of Secret (without categories), Rmin 2 and Rmax 3.

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 system users" is more accurately stated as "maximum

clearance of the least cleared system user." For simplicity, this document uses the former phrase.

2 There is one anomalous case in which this formula gives an incorrect result This is the case where the minimum clearance is Top Secret/Background Investigation and the maximum data sensitivity is Top Secret. According to the formula, this gives a risk index of l. In actuality, the risk index in this case is zero. The anomaly results because there are two "levels" of Top Secret clearance and only one level of Top Secret data.

TABLE 1

RATING SCALE FOR MINIMUM USER CLEARANCE[1]

MINIMUM USER CLEARANCE	RATING
Uncleared (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret(S)	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 See Appendix B for a detailed description of the terms listed

TABLE 2

RATING SCALE FOR MAXIMUM DATA SENSITIVITY

MAXIMUM DATA SENSITIVITY RATINGS 2 WITHOUT CATEGORIES (Rmax)	RATING (Rmax)	MAXIMUM DATA SENSITIVITY WITH CATEGORIES1	
Unclassified (U)	0	Not Applicable3	
Not Classified but Sensitives4	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)	55	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 to the category. 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 imply sensitivity of data and unclassified data is not sensitive, unclassified data by definition cannot contain categories.

4 N data includes financial, proprietary, privacy, and mission sensitive data. Some situations (e.g., those involving extremely large financial sums or critical mission sensitive data), may warrant a higher rating. 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)

TABLE 3
SECURITY RISK INDEX MATRIX

Maximum Data Sensitivity

		U	N	C	S	TS	1C	MC
	U	0	1	2	3	4	5	6
	N	0	0	1	2	4	5	6
Minimum	C	0	0	0	1	3	4	5
Clearance or	S	0	0	0	0	2	3	4
Authorization of	TS(BI)	0	0	0	0	0	2	3
System Users	TS(SBI)	0	0	0	0	0	1	2
	1C	0	0	0	0	0	0	1
	MC	0	0	0	0	0	0	0

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS(SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Categories

In situations where the local environment indicates that additional risk factors are present, a larger risk index may be warranted. Table 2 and the above discussion show how the presence of nonhierarchical sensitivity categories such as NOFORN (Not Releasable to Foreign Nationals) and PROPIN (Caution- Proprietary Information Involved) influences the ratings.(14) Compartmented information is also encompassed by the term sensitivity categories as is information revealing sensitive intelligence sources and methods. A' subcategory (and a subcompartment) is considered to be independent from the category to which it is subsidiary.

Table 3 presents a matrix summarizing the risk' indices corresponding to the various clearance/sensitivity pairings. For simplicity no categories are associated with the maximum data sensitivity levels below Top Secret.

3.0 COMPUTER SECURITY REQUIREMENTS FOR OPEN SECURITY ENVIRONMENTS

This section discusses the application of the Computer Security Requirements to systems in open security environments. An open security environment is one in which system applications are not adequately protected against the insertion of malicious logic. Appendix C describes malicious logic and the open security environment in more detail.

3.1 Recommended Classes

Table 4 presents the minimim evaluation class identified in the Computer Security Requirements for different risk indices in an open security environment. Table 5 illustrates the impact of the requirements on individual minimum clearance/maximum data sensitivity pairings, where no categories are associated with maximum data sensitivity below Top Secret. The minimum evaluation class is determined by finding the matrix entry corresponding to the minimum clearance or authorization of system users and the maximum sensitivity of data processed by the system.

> Example: If the minimum clearance of system users is Secret and the maximum sensitivity of data processed is Top Secret (with no categories), then the risk index is 2 and a class B2 system is required.

The classes identified are minimum values. Environmental characteristics must be examined to determine whether a higher class is warranted. Factors that might argue for a higher evaluation class include the following:

a. High volume of information at the maximum data sensitivity.

b. Large number of users with minimum clearance.

Both of these factors are often present in networks.

The guidance embodied in the Computer Security Requirements is best used during system requirements definition to determine which class of trusted system is required given the risk index envisioned for a specific environment. They are also of use in determining which choices are feasible given either the maximum sensitivity of data to be processed or minimum user clearance or authorization requirements. The Computer Security Requirements can also be used in a security evaluation to determine whether system safeguards are sufficient.

3.2 Risk index and Operational Modes

Situations with a risk index of zero encompass systems operating in system high or dedicated mode. Systems operating in dedicated mode--in which all users have both the clearance and the need-to-know for all information in the system--do not need to rely on hardware and software protection measures for security.(10) Therefore, no minimum level of trust is prescribed. However, because of the integrity and denial of service requirements of many systems, additional protective features may be warranted.

TABLE 4

COMPUTER SECURITY REQUIREMENTS FOR OPEN SECURITY ENVIRONMENTS

RISK INDEX	SECURITY OPERATING MODE	MINIMUM CRITERIA CLASS1
0	Dedicated	No Prescribed Minimum2
0	System High	C23
1	Limited Access, Controlled, Compartmented, Multilevel	B14
2	Limited Access, Controlled, Compartmented, Multilevel	B2
3	Controlled, Multilevel	B3
4	Multilevel	A1
5	Multilevel	*
6	Multilevel	*
7	Multilevel	*

1 The asterisk (*) indicates that computer protection for environments with that risk index are considered to be beyond the state of current technology. Such environments must augment technical protection with personnel or administrative security safeguards.

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

3 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.

4 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.

TABLE 5

SECURITY INDEX MATRIX FOR OPEN SECURITY ENVIRONMENTS[1]

		Maximum Data Sensitivity						
		U	N	C	S	TS	1C	1M
	U	C1	B1	B2	B3	*	*	*
Minimum	N	C1	C2	B2	B2	A1	*	*
Clearance or	C	C1	C2	C2	B1	B3	A1	*
Author- ization	S	C1	C2	C2	C2	B2	B3	A1
of System Users	TS(BI)	C1	C2	C2	C2	C2	B2	B3
	TS(SBI)	C1	C2	C2	C2	C2	B1	B2
	1C	C1	C2	C2	C2	C2	C2[2]	B1[3]
	MC	C1	C2	C2	C2	C2	C2[2]	C2[2]

1 Environments for which either C1 or C2 is given are for systems that operate in system high mode. No minimum level of trust is prescribed for systems that operate in dedicated mode. Categories are ignored in the matrix, except for their inclusion at the TS level.

2 It is assumed that all users are authorized access to all categories present in the system. If some users are not authorized for all categories, then a class B1 system or higher is required.

3 Where there are more than two categories, at least a class B2 system is required.

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS(SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Category

In system high mode, all users have sufficent security clearances and category authorizations for all data, but some users do not have a need-to-know for all information in the system.(10) Systems that operate in system high mode thus are relied on to protect information from users who do not have the appropriate need-to-know. Where classified or sensitive unclassified data is involved, no less than a class C2 system is allowable due to the need for individual accountability.

In accordance with policy, individual accountability requires that individual system users be uniquely identified and an automated audit trail kept of their actions. Class C2 systems are the lowest in the hierarchy of trusted systems to provide individual accountability and are therefore required where sensitive or classified data is involved. The only case where no sensitive or classified data is involved is the case in which the maximum sensitivity of data is unclassified. In this case, hardware and software controls are still required to allow users to protect project or private information and to keep other users from accidentally reading or destroying their data. However, since there is no officially sensitive data involved, individual accountability is not required and a class C1 system suffices. In system high mode sensitivity labels are not required for making access control decisions. In this mode access is based on the need-to-know, which is based on permissions (e.g., group A has access to file A), not on sensitivity labels. The type of access control used to provide need-to-know protection is called discretionary access control. It is defined as a means of restricting access to objects based on the identity of subjects and/or groups to which the subjects belong. All systems above Division D provide discretionary access control mechanisms. These mechanisms are more finely grained in class C2 systems than in Class C1 systems in that they provide the capability of including or excluding access to the granularity of a single user. Division C systems (C1 and C2) do not possess the capability to provide trusted labels on output. Therefore, output from these systems must be labeled at the system high level and manually reviewed by a responsible individual to determine the correct sensitivity prior to release beyond the perimeter of the system high protections of the system.(10)

Environments with a risk index of 1 or higher encompass systems operating in controlled, compartmented, and multilevel modes. These environments require mandatory access control, which is the type of access control used to provide protection based on sensitivity labels. It is defined as a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal clearance or authorization of subjects to access information of such sensitivity. Division B and A systems provide mandatory access control, and are therefore required for all environments with risk indices of 1 or greater.

The need for internal labeling has a basis in policy, in that DoD Regulation 5200.1-R requires computer systems that process sensitive or classified data to provide internal classification markings.(3) Other requirements also exist.

> Example: The DCID entitled "Security Controls on the Dissemination of Intelligence Information" requires that security control markings be "associated (in full or abbreviated form) with data stored or processed in automatic data processing systems."(14)

Sensitivity labeling is also required for sensitive unclassified data.(15,16)

> Example: Data protected by Freedom of Information (FOI) Act exemptions must be labeled as being "exempt from mandatory disclosure under the FOI Act."(15)

This example illustrates not only the need for labeling but also the fact that the purpose of FOI Act exemptions is to provide access control protection for sensitive data. In summary, it is a required administrative security practice that classified and unclassified sensitive information be labeled and controlled based on the labels. It follows that prudent computer security practice requires similar labeling and mandatory access control.

The minimum class recommended for environments requiring mandatory access control is class B1, since class B1 systems are the lowest in the hierarchy of trusted systems to provide mandatory access control.

> Example: Where no categories are involved, systems with minimum clearance/maximum data sensitivity pairings of U/N and C/S have a risk index of 1 and thus require at least a class B1 system.

Some systems that operate in system high mode use mandatory access control for added protection within the system high environment, even though the controls are not relied upon to properly label and protect data passing out of the system high environment. There has also been a recommendation that mandatory access controls (i.e., class B1 or higher systems) be used whenever data at two or more sensitivity levels is being processed, even if everyone is fully cleared, in order to reduce the likelihood of mixing data from files of higher sensitivity with data of files of lower sensitivity and releasing the data at the lower sensitivity.(17) These points reaffirm the fact that the classes identified in the requirements are minimum values.

This report emphasizes that output from a system operating in system high mode must be stamped with the sensitivity and category labels of the most sensitive data in the system until the data is examined by a responsible individual and its true sensitivity level and category are determined. If a system can only be trusted for system high operation, its labels cannot be assumed to accurately reflect data sensitivity. The use of division B or A systems does not necessarily solve this problem.

> Example: Take the case of a system in an open security environment that processes data classified up to Secret and supports some users who have only Confidential clearances. According to the requirements, such a situation represents a risk index of 1 and thus requires a class B1 system. Some of the reports produced by the system might be unclassified. Nevertheless, such a report cannot be forwarded to uncleared people until the report is examined and its contents determined to be unclassified. Without the existence of such a review, the recipient becomes an indirect user and the risk index becomes 3. A class B1 system no longer provides adequate data protection. Therefore, even though the system is trusted to properly label and segregate Confidential and Secret data, it is not simultaneously trusted to properly label and segregate unclassified data.

Systems with a risk index of 2 require more trust than can be placed in a class B1 system. Where no categories are involved, class B2 systems are the minimum required for minimum clearance/maximum data sensitivity pairings such as U/C, N/S and S/TS, all of which have a risk index of 2. Class B2 systems have several characteristics that justify this increased trust:

a. The Trusted Computing Base (TCB) is carefully structured into protection-critical and nonprotection-critical elements. The TCB interface is well defined, and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review.

b. The TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class B1 systems to be extended to all subjects and objects in the system. That is, security rules are more rigorously defined and have a greater influence on system design.

c. Authentication mechanisms are strengthened, making it more difficult for a malicious user or malicious software to improperly intervene in the login process.

d. Stringent configuration management controls are imposed for life-cycle assurance.

e. Covert channels are addressed to defend against their exploitation by malicious software.(18) A covert channel is a communication channel that violates the system's security policy.

Because of these and other characteristics, class B2 systems are relatively resistant to penetration. A risk index of 3, however, requires greater resistance to penetration. Class B3 systems are highly resistant to penetration and are the minimum required for situations with a risk index of 3 such as those with minimum clearance/maximum data sensitivity pairings of U/S, C/TS, S/TS with one category, and TS(BI)/TS with multiple categories. Characteristics that distinguish class B3 from class B2 systems include the following:

a. The TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. Much effort is thus spent on minimizing TCB complexity.

b. Enhancements are made to system audit mechanisms and system recovery procedures.

c. Security management functions are performed by a security administrator rather than a system administrator.

While several new features have been added to class B3 systems, the major distinction between class B2 and class B3 systems is the increased trust that can be placed in the TCB of a class B3 system. The most trustworthy systems defined by the Criteria are class Al systems. Class Al systems can be used for situations with a risk index of 4, such as the following minimum clearance/maximum data sensitivity pairings: N/TS, C/TS with one category, and S/TS with multiple categories. Class Al systems are functionally equivalent to those in class B3 in that no additional architectural features or policy requirements are added. The distinguishing characteristic of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. In addition, more stringent configuration management is required and procedures are established for securely distributing the system to sites.

The capability to support systems in open security environments with a risk index of 5 or greater is considered to be beyond the state-of-the-art. For example, technology today does not provide adequate security protection for an open environment with uncleared users and Top Secret data. Such environments must rely on physical, personnel, or information security solutions or on such technical approaches as periods processing.

4.0 COMPUTER SECURITY REQUIREMENTS FOR CLOSED SECURITY ENVIRONMENTS

This section discusses the application of the Computer Security Requirements to systems in closed security environments. A closed security environment is one in which system applications are adequately protected against the insertion of malicious logic. Appendix C describes the closed security environment in more detail. The main threat to the TCB from applications in this environment is not malicious logic, but logic containing unintentional errors that might be exploited for malicious purposes. As system quality reaches class B2, the threat from logic containing unintentional errors is substantially reduced. This reduction permits the placement of increased trust in class B2 systems due to (1) the increased attention that B2 systems give to the interface between the application programs and the operating system, (2) the formation of a more centralized TCB, and (3) the elimination of penetration flaws. Nevertheless, the evaluation class of B1 assigned for open security environments cannot be reduced to a class C1 or C2 in closed security environments because of the requirement for mandatory access controls.

Table 6 presents the minimum evaluation class identified in the Computer Security Requirements for different risk indices in a closed security environment. The principal difference between the requirements for the open and closed environments is that in closed environments class B2 systems are trusted to provide sufficient protection for a greater risk index. As a result, environments are supportable that were not supportable in open situations (e.g., uncleared user on a system processing Top Secret data). Table 7 illustrates the requirements' impact on individual minimum clearance/maximum data sensitivity pairings.

TABLE 6

COMPUTER SECURITY REQUIREMENTS FOR CLOSED SECURITY ENVIRONMENTS

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

1 The asterisk (*) indicates that computer protection for environments with that risk index are considered to be beyond the state of current technology. Such environments must augment technical protection with physical, personnel, and/or administrative safeguards.

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

3 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.

–Where a system processes classified or compartmented data and some users do not have at least a Confidential clearance, at least a class B2 system is required.

TABLE 7
SECURITY INDEX MATRIX FOR CLOSED SECURITY ENVIRONMENTS[1]

		Maximum Data Sensitivity						
		U	N	C	S	TS	1C	MC
	U	C1	B1	B2	B2	A1	*	*
Minimum	N	C1	C2	B1	B2	B3	A1	*
Clearance or	C	C1	C2	C2	B1	B2	B3	A1
Author-	S	C1	C2	C2	C2	B2	B2	B3
ization	TS(BI)	C1	C2	C2	C2	C2	B2	B2
of System	TS(SBI)	C1	C2	C2	C2	C2	B1	B2
Users	1C	C1	C2	C2	C2	C2	C2[2]	B1[3]
	MC	C1	C2	C2	C2	C2	C2[2]	C2[2]

1 Environments for which either C1 or C2 is given are for systems that operate in system high mode. There is no prescribed minimum level of trust for systems that operate in dedicated mode. Categories are ignored in the matrix, except for their inclusion at the TS level.

2 It is assumed that all users are authorized access to all categories on the system. If some users are not authorized for all categories, then a class B1 system or higher is required.

3 Where there are more than two categories, at least a class B2 system is required.

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive UnclassiFied Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS (SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Categories

APPENDIX A

SUMMARY OF CRITERIA The DoD Trusted Computer System Evaluation Criteria(4) provides a basis for specifying security requirements and a metric with which to evaluate the degree of trust that can be placed in a computer system. These criteria are hierarchically ordered into a series of evaluation classes where each class embodies an increasing amount of trust. A summary of each evaluation class is presented in this appendix. This summary should not be used in place of the Criteria. The evaluation criteria are based on six fundamental security requirements that deal with controlling access to information. These requirements can be summarized as follows:

a. Security policy--There must be an explicit and well-defined security policy enforced by the system.

b. Marking--Access control labels must be associated with objects.

c. Identification--Individual subjects must be identified.

d. Accountability--Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.

e. Assurance--The computer system must contain hardware and software mechanisms that can be evaluated independently to provide sufficient assurance that the system enforces the security policy.

f. Continuous protection--The trusted mechanisms that enforce the security policy must be protected continuously against tampering and unauthorized changes.

The evaluation criteria are divided into four divisions--D, C, B, and A; divisions C, B, and A are further subdivided into classes. Division D represents minimal protection, and class A1 is the most trustworthy and desirable from a computer security point of view.

The following overviews are excerpts from the Criteria:

Division D: Minimal Protection. This division contains only one class. It is reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation class.

Division C: Discretionary Protection. Classes in this division provide for discretionary (need-to-know) protection and accountability of subjects and the actions they initiate, through inclusion of audit capabilities.

Class C1: Discretionary Security Protection. The TCB of class C1 systems nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of, credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class C I environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Class C2: Controlled Access Protection. Systems in this class enforce a more finely grained discretionary access control than class C1 systems, making users individually accountable for their actions through logic procedures, auditing of security-relevant events, and resources encapsulation.

Division B: Mandatory Protection. The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Class B1: Labeled Security Protection. Class B1 systems require all the features required for class C2. In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

Class B2: Structured Protection. In class B2 systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in B1 systems be extended to all subjects and objects in the system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and nonprotection-critical elements. The TCB interface is well defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for systems administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

Class B3: Security Domains. The class B3 TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant software engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

Division A: Verified Protection. This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect the classified and other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development, and implementation.

Class A1: Verified Design. Systems in class A1 are functionally equivalent to those in class B3 in that no additional architectural features or policy requirements have been added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature starting with a formal model of security policy and a formal top-level specification (FTLS) of the design. In keeping with the extensive design and development analysis of the TCB required of systems in class A1, more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

APPENDIX B

DETAILED DESCRIPTION OF CLEARANCES AND DATA SENSITIVITIES

This appendix describes in detail the clearances and data sensitivities (e.g., classification) introduced in the body of the report.

B.1 Clearances

This section defines increasing levels of clearance or authorization of system users. System users include not only those users with direct connections to the system but also those users without direct connections who might receive output or generate input that is not reliably reviewed for classification by a responsible individual.

a. Uncleared (U)--Personnel with no clearance or authorization. Permitted access to any information for which there are no specified controls, such as openly published information.

b. Unclassified Information (N)--Personnel who are authorized access to sensitive unclassified (e.g., For Official Use Only (FOUO)) information, either by an explicit official authorization or by an implicit authorization derived from official assignments or responsibilities.(15)

c. Confidential Clearance (C)--Requires U.S. citizenship and typically some limited records checking.(19) In some cases, a National Agency Check (NAC) is required (e.g., for U.S. citizens employed by colleges or universities).(20)

d. Secret Clearance (S)--Typically requires a NAC, which consists of searching the Federal Bureau of Investigation fingerprint and investigative files and the Defense Central Index of Investigations.(19) In some cases, further investigation is required.

e. Top Secret Clearance based on a current Background Investigation (TS(BI))--Requires an investigation that consists of a NAC, personal contacts, record searches, and written inquiries. A B1 typically includes an investigation extending back 5 years, often with a spot check investigation extending back 15 years.(19)

f. Top Secret Clearance based on a current Special Background Investigation (TS(SBI))--Requires an investigation that, in addition to the investigation for a B1, includes additional checks on the subject's immediate family (if foreign born) and spouse and neighborhood investigations to verify each of the subject's former residences in the United States where he resided six months or more. An SBI typically includes an investigation extending back 15 years.(19)

g. One category (1C)1 - In addition to a TS(SBI) clearance, written authorization for access to one category of information is required. Authorizations are the access rights granted to a user by a responsible individual (e.g., security officer).

h. Multiple categories (MC)' - In addition to TS(SBI) clearance, written authorization for access to multiple categories of information is required.

The extent of investigation required for a particular clearance varies based both on the background of the individual under investigation and on derogatory or questionable information disclosed during the investigation. Identical clearances are assumed to be equivalent, however, despite differences in the amount of investigation peformed.

Individuals from non-DoD agencies might be issued DoD clearances if the clearance obtained in their agency can be equated to a DoD clearance. For example, the "Q" and "L" clearances granted by both the Department of Energy and the Nuclear Regulatory Commission are considered acceptable for issuance of a DoD industrial personnel security clearance.(20) The "Q" clearance is considered an authoritative basis for a DoD Top Secret clearance (based on a B1) and the "L" clearance is considered an authoritative basis for a DoD Secret clearance.(20)

Foreign individuals might be granted access to classified U.S. information although they do not have a U.S. clearance. Access to classified information by foreign nationals, foreign governments, international organizations, and immigrant aliens is addressed by National Disclosure Policy, DoD Directive 5230.11, and DoD Regulation 5200.I-R.(3,21,22) The minimum user clearance rating table applies in such cases if the foreign clearance can be equated to one of the clearance or authorization levels in the table.

B.2 Data Sensitivities

Increasing levels of data sensitivity are defined as follows:

a. Unclassified (U)--Data that is not sensitive or classified: publicly releasable information within a computer system. Note that such data might still require discretionary access controls to protect it from accidental destruction.

b. Not Classified but Sensitive (N)--Unclassified but sensitive data. Much of this is FOUO data, which is that unclassified data that is exempt from release under the Freedom of Information Act.(15) This includes data such as the following:

   I. Manuals for DoD investigators or auditors.

1 These are actually authorizations rather than clearance levels, but they are included here to emphasize their importance.

2. Examination questions and answers used in determination of the qualification of candidates for employment or promotion.

3. Data that a statute specifically exempts from disclosure, such as Patent Secrecy data.(23)

4. Data containing trade secrets or commercial or financial information.

5. Data containing internal advice or recommendations that reflect the decision-making process of an agency.(24)

6. Data in personnel, medical, or other files that, if disclosed, would result in an invasion of personal privacy.(25)

7. Investigative records.

   DoD Directive 5400.7 prohibits any material other than that cited in FOI Act exemptions from being considered or marked FOUO.(15) One other form of unclassified sensitive data is that pertaining to unclassified technology with military application.(16) This refers primarily to documents that are controlled under the Scientific and Technical Information Program or acquired under the Defense Technical Data Management Program.(26,27) In addition to specific requirements for protection of particular forms of unclassified sensitive data, there are two general mandates. The first is Title 18, U.S. Code 1905, which makes it unlawful for any office or employee of the U.S. Government to disclose information of an official nature except as provided by law, including when such information is in the form of data handled by computer systems.(28) Official data is data that is owned by, produced by or for, or is under the control of the DoD. The second is Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum Number I, which establishes requirements for Federal agencies to protect sensitive data.(30)

c. Confidential (C)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.(3)

d. Secret (S)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.(3)

e. Top Secret (TS)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.(3)

f. One Category (1C)2--Applied to Top Secret Special Intelligence information (e.g., Sensitive Compartmented Information (SCI) or operational information (e.g., Single Integrated Operational Plan/Extremely Sensitive Information (SIOP/ESI)) that requires special controls for restrictive handling.(3) Access to such information requires authorization by the office responsible for the particular compartment. Compartments also exist at the C and 5 levels (see the discussion below).

g. Multiple Categories (MC)2--Applied to Top Secret Special Intelligence or operational information that requires special controls for restrictive handling. This sensitivity level differs from the 1C level only in that there are multiple compartments involved. The number can vary from two to many, with corresponding increases in the risk involved.

Data sensitivity groupings are not limited to the hierarchical levels discussed in Section B.2. Nonhierarchical sensitivity categories such as NOFORN and PROPIN are also used.(14) Compartmented information is also included under the term sensitivity categories, as is information revealing sensitive intelligence sources and methods. Other sources of sensitivity categories include (a) the Atomic Energy Act of 1954, (b) procedures based on International Treaty requirements, and (c) programs for the collection of foreign intelligence or under the jurisdiction of the National Foreign Intelligence Advisory Board or the National Communications Security Subcommittee.(11,32,33,34,35) Such nonhierarchical sensitivity categories can occur at each hierarchical sensitivity level.

2 These are actually categories rather than classification levels. They are included here to emphasize their importance.

APPENDIX C

ENVIRONMENTAL TYPES The amount of computer security required in a system depends not only on the risk index (Section 2) but also on the nature of the environment. The two environmental types of systems defined in this document are based on whether the applications that are processed by the TCB are adequately protected against the insertion of malicious logic. A system whose applications are not adequately protected is referred to as being in an open environment. If the applications are adequately protected, the system is in a closed environment. The presumption is that systems in open environments are more likely to have malicious application than systems in closed environments. Most systems are in open environments.

Before defining the two environmental categories in more detail, it is necessary to define several terms.

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

b. Application. Those portions of a system, including portions of the operating system, that are not responsible for enforcing the systems security policy.

c. Malicious Logic. Hardware, software, or firmware that is intentionally included for the purpose of causing loss or harm (e.g., Trojan horses).

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

C.1 Open Security Environment

Based on these definitions, an open security environment includes those systems in which either of the following conditions holds true:

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

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

Configuration control, by the broad definition above, encompasses all factors associated with the management of changes to a system. For example, it includes the factor that the application's user interface might present a sufficiently extensive set of user capabilities such that the user cannot be prevented from entering malicious logic through the interface itself.

In an open security environment, the malicious application logic that is assumed to be present can attack the TCB in two ways. First, it can attempt to thwart TCB controls and thereby "penetrate" the system. Secondly, it can exploit covert channels that might exist in the TCB. This distinction is important in understanding the threat and how it is addressed by the features and assurances in the Criteria.

C.2 Closed Security Environment

A closed security environment includes those systems in which both of the following conditions hold true:

a. Applications developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic.

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

Clearances are required for assurance against malicious applications logic because there are few other tools for assessing the security-relevant behavior of application hardware and software. On the other hand, several assurance requirements from the Criteria help to provide confidence that the TCB does not contain malicious logic. These assurance requirements include extensive functional testing, penetration testing, and correspondence mapping between a security model and the design. Application logic typically does not have such stringent assurance requirements. Indeed, typically it is not practical to build all application software to the same standards of quality required for security software.

The configuration control condition implicitly includes the requirement that users be provided a sufficiently limited set of capabilities to pose an acceptably low risk of entering malicious logic. Examples of systems with such restricted interfaces might include those that offer no data sharing services and permit the user only to execute predefined processes that run on his behalf, such as message handlers, transaction processors, and security "filters" or "guards."

GLOSSARY

For additional definitions, refer to the Glossary in the DoD Trusted Computer System Evaluation Criteria.(4)

Application

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

Category

A grouping of classified or unclassified but sensitive information, to which an additional restrictive label is applied (e.g., proprietary, compartmented information).

Classification

A determination that information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made. (Adapted from DoD Regulation 5200.I-R.)(3) Data classification is used along with categories in the calculation of risk index.

Closed Security Environment

An environment that includes those systems in which both of the following conditions hold true:

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

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

Compartmented Information

Any information for which the responsible Office of Primary Interest (OPI) requires an individual needing access to that information to possess a special authorization.

Configuration Control

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

Covert Channel

A communications channel that allows a process to transfer information in a manner that violates the system's security policy.(4)

Discretionary Access Control

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.(4)

Environment

The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. (See Open Security Environment and Closed Security Environment.)

Label

Apiece of information that represents the security level of an object and that describes the sensitivity of the information in the object.

Malicious Logic

Hardware, software, or firmware that is intentionally included in a system for the purpose of causing loss or harm.

Mandatory Access Control

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.(4)

Need-To-Know

A determination made by the processor of sensitive information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of the sensitive information in order to perform official tasks or services. (Adapted from DoD Regulation 5220.22-R.)(20)

Open Security Environment

An environment that includes those systems in which one of the following conditions holds true:

a. Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic. (See the definition of Closed Security Environment for an explanation of sufficient clearance.)

b. 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 classification of data processed by the 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.(4)

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 Users

Users 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 the risk index.

ACRONYMS

A1	An evaluation class requiring a verified design
ADP	Automated Data Processing
ADPS	Automated Data Processing System
AFSC	Air Force Systems Command
B1	An Evaluation class requiring labeled security protection
B2	An Evaluation class requiring structured protection
B3	An evaluation class requiring security domains
BI	Background Investigation
C	Confidential
C1	An evaluation class requiring discretionary access protection
C2	An evaluation class requiring controlled access protection
CI	Compartmented Information
CSC	Computer Security Center
COMINT	Communications Intelligence
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DIAM	Defense Intelligence Agency Manual
DIS	Defense Investigative Service
DoD	Department of Defense
DoDCSC	Department of Defense Computer Security Center
ESD	Electronic Systems Division
FOI	Freedom of Information
FOUO	For Official Use Only
FTLS	Formal Top-Level Specification
IEEE	Institute of Electrical and Electronics Engineers
L	A personnel security clearance granted by the Department of Energy and the Nuclear Regulatory Commission
MC	Multiple Compartments
N	Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
NAC	National Agency Check
NATO	North Atlantic Treaty Organization
NOFORN	Not Releasable to Foreign Nationals
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NTIS	National Technical Information Service
OMB	Office of Management and Budget
OPI	Office of Primary Interest
OPNAV	Office of the Chief of Naval Operations
OSD	Office of the Secretary of Defense

PRO PIN	Caution--Proprietary Information Involved
Q	A personnel security clearance granted by the Department of Energy and the Nuclear Regulatory Commission
S	Secret
SBI	Special Background Investigation
SCI	Sensitive Compartmented Information
SIOP	Single Integrated Operational Plan
SIOP-ESI	Single Integrated Operational Plan--Extremely Sensitive Information
SM	Staff Memorandum
STD	Standard
TCB	Trusted Computing Base
TS	Top Secret
U	Uncleared or Unclassified
U.S.	United States
IC	One Compartment

REFERENCES

1. DoD Computer Security Center, Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-003-85, 25 June 1985.

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

3. DoD Regulation 5200.1-R, Information Security Program Regulation, August 1982.

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

5. Army Regulation 380-380, Automated Systems Security, IS June 1979.

6. Office of the Chief of Naval Operations (OPNAV) Instruction 5239. IA "Department of the Navy Automatic Data Processing Security Program," 3' August 1982.

7. Air Force Regulation 205-16, Automated Data Processing System (ADPS) Security Policy, Procedures, and Responsibilities, I August 1984.

8. Marine Corps Order P5510.14, Marine Corps Automatic Data Processing (ADP) Security Manual, 4 November 1982.

9. DoD Directive 5220.22, "DoD Industrial Security Program," 8 December 1980.

10. DoD Directive 5200.28, "Security Requirements for Automatic Data Processing Systems," 29 April 1978.

11. DoD Manual 5200.28-M, ADP Security Manual - Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, 25 June 1979.

12. Defense Intelligence Agency Manual (DIAM) 50-4, "Security of Compartmented Computer Operations (U)," 24 June 1980, CONFIDENTIAL.

13. National Security Agency/Central Security Service (NSA/CSS) Directive 10-27, "Security Requirements for Automatic Data Processing (ADP) Systems," 29 March 1984.

14. Director of Central Intelligence Directive (DCID), "Security Controls on the Dissemination of Intelligence Information (U)," 7 January 1984, CONFIDENTIAL.

15. DoD Directive 5400.7, "DoD Freedom of Information Act Program," 24 April 1980.

16. Office of the Secretary of Defense (OSD) Memorandum, "Control of Unclassified Technology with Military Application," 18 October 1983.

17. Anderson, James P., "An Approach to Identification of Minimum TCB Requirements for Various Threat/Risk Environments," Proceedings of the 1983 IEEE Symposium on Security and Privacy, 24-27 April 1983.

18. Schell, Roger R., "Evaluating Security Properties of Systems," Proceedings of the IEEE Symposium on Security and Privacy, 24-27 April 1983.

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

20. DoD Regulation 5220.22-R, Industrial Security Regulation, January 1983.

21. National Disclosure Policy - I, 9 September 1981.

22. DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," 31 December 1976.

23. Title 35, United States Code, Section 181-188, "Patent Secrecy."

24. Title 5, United States Code, Section 551, "Administrative Procedures Act."

25. DoD Directive 5400.11, "Department of Defense Privacy Program," 9 June 1982.

26. DoD Directive 5100.36, "Defense Scientific and Technical Information Program," 2 October 1981.

27. DoD Directive 5010.12, "Management of Technical Data," 5 December 1968.

28. Title 18, United States Code, Section 1905, "Disclosure of Confidential Information Generally."

29. DoD Directive 5200.1, "DoD Information Security Program," 7 June 1982.

30. Office of Management and Budget (OMB) Circular No. A-71, Transmittal Memorandum No. I, "Security of Federal Automated Information Systems, 27 July 1978.

31. Joint Chiefs of Staff (JCS) Staff Memorandum (SM) 313-83, Safeguarding the Single Integrated Operational Plan (SIOP) (U), 10 May 1983, SECRET.

32. "Security Policy on Intelligence Information in Automated Systems and Networks (U)," Promulgated by the DCI, 4 January 1983, CONFIDENTIAL.

33. Director of Central Intelligence Computer Security Manual (U), Prepared for the DCI by the Security Committee, 4 January 1983, CONFIDENTIAL.

34. DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," 12 January 1978.

35. DoD Instruction C-5210.21, "Implementation of NATO Security Procedure (U)," 17 December 1973, CONFIDENTIAL.