

ATTACHMENT 7

Table of Contents

PARA	TITLE	PAGE
1	General System Security Requirements	3
2	General Design Requirements	4
3	Operational Level Computer Security Requirements	4
4	Trusted Computing Base Security Requirements	9
5	Assurance Controls for TCB Development	21

(This page intentionally blank)

ATTACHMENT 7

SYSTEM\_SECURITY\_REQUIREMENTS\_C2\_and\_B1\_LEVEL

12 June 1991

1 General System Security Requirements.

All requirements apply to C2 level and higher Trusted Computing Base (TCB) systems unless otherwise marked.

1.1 DOD Policy. The system shall be developed in compliance with current DOD policy concerning protection of classified information. The policy deals with authorizations to access information by a user based on the user's security clearance and the information's security label. The security policies are contained in:

- a. Information Security Program Regulation (DOD Regulation 5200.1-R and AFR 205-1);

- b. Security Requirements for ADP Systems (DOD Directive 5200.28);
- c. ADP Security Manual - Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems (DOD Manual 5200.28-M and AFR 205-16);
- d. Industrial Security Manual for Safeguarding Classified Information (DOD Manual 5220.22-M);
- e. National Security Information (Executive Order 12356);
- f. DOD Password Management Guidelines (CSC-STD-002-85).
- g. Guidance for security of Federal automated system is found in OMB Circular A-130.
- h. Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX system (NCSC-TG-020-A Version-1).

1.2 Security Label. The security label of a unit of information (object) shall consist of mandatory and discretionary security attributes.

1.3 Discretionary Security. The discretionary security attributes of the information shall consist of need-to-know access permission assignments (e.g. assignments of groups or specific individuals and their respective modes of access to the information) for the system users. The multiuser systems shall support at least 1000 need-to-know groups with 400 subjects per group. The single user systems shall support at least 10 need-to-know groups.

1.4 System High. The system shall operate in system high mode in accordance with (IAW) DOD Directive 5200.28 and AFR 205-16.

1.5 (B1 level and higher) Security Clearance. A user security clearance shall consist of hierarchical personnel security clearance or authorization (e.g. Top Secret, Secret), nonhierarchical security compartment clearances or authorizations, and necessary biographical user data (e.g. U.S. or foreign citizen, Government employee, Contractor employee, etc.) to determine applicability of the mandatory security attributes of the information to be accessed.

1.6 (B1 level AF1 and higher) Mandatory Security Attributes. The mandatory security attributes of the information shall consist of hierarchical classification level (e.g. Secret, Top Secret, Unclassified) and nonhierarchical security compartments or categories (e.g. SI, TK, SIOP, FOUO).

1.7 (B1 level and higher) Multilevel Security. The system shall operate in multilevel security mode IAW DOD Directive 5200.28 and AFR 205-16. Application software shall also support multilevel security processing.

## 2 General Design Requirements.

2.1 Trusted Computing Base. The system security requirements are stated in terms of the security requirements for the system's computing base. The computing base of the system, which is security relevant, shall be trustable and shall be called the system's TCB. The TCB shall consist of all the system's relevant security hardware, firmware, and software. Further TCB details are provided later. The TCB capabilities shall be an integral part of

the total system solution. The TCB shall not be developed independently from the other requirements. The TCB shall be developed along with the other functional needs of the system.

2.2 Individual Accountability. The TCB shall enforce individual accountability.

2.3 Secure Access Control. The TCB shall include secure access control mechanisms that prevent:

- a. Unauthorized disclosure (compromise) of classified information;
- b. Unauthorized alteration (data integrity) of information processed by the system;
- c. Unauthorized alteration (system integrity) of the TCB.

### 3 Operational Level Computer Security Requirements.

Effective operational level computer security requirements the system must fulfill shall be applicable to the testing and verification of the system's TCB. This requirement is concerned with how the system as a whole effectively operates to support and complement the procedural security policy of the sites where systems shall be installed.

3.1 Operational Level Requirements. The following basic computer security requirements are derived for the system from regulations and security policy specified in paragraph 1 and the DOD Trusted Computer System Evaluation Criteria document (DOD 5200.28-STD). These requirements shall be applicable for the TCB, and shall apply for the development and operation (multilevel operation for B1 and higher TCB) of the system.

3.2 (B1 level and higher) Labels. The TCB shall preserve sensitivity labels associated with each subject and storage object under its control.

#### 3.2.1 (B1 level and higher) Sensitivity.

3.2.1.1 (B1 level and higher) The TCB shall ensure sensitivity labels accurately represent the security level of specified subjects and objects. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported. To import non-labeled data, the TCB shall request and receive the security level of the data from an authorized user.

3.2.2 (B1 level and higher) Usage. The labels of information shall be used as the basis for access control decisions.

3.3 (B1 level and higher) Mandatory\_Security. The TCB shall enforce control of information based on security classification level, security compartments, and security clearances with users requesting or creating classified information.

3.3.1 (B1 level and higher) Read Access. A subject may be permitted read access to an object if the subject's security level dominates the object's security level and is authorized access based on need-to-know.

3.3.2 (B1 level and higher) Write\_Access. A subject may be permitted

write access to an object if the object's security level dominates the subject's security level and is authorized write access based on need-to-know.

3.4 Discretionary Security. The TCB shall enforce need-to-know access restrictions placed on information managed by the system. The need-to-know access restrictions for information when created or changed shall be determinable by the office of primary responsibility or the originator of the information. Only users who are determined to have a "need-to-know" for information (and who have legitimate access to the information based on clearance) shall have the capability to access the information.

3.4.1 Identification. The TCB shall require users to identify themselves to it before performing any other actions the TCB is expected to mediate. Identification and authorization data shall be used by the TCB to determine user access to information (and shall be associated with every active element performing a security relevant action). User identification and authorization data and sensitivity labels of resources associated with the system (e.g. terminals, access lines) shall be initially established and subsequently protected by the system's security administrator, and shall be managed by the TCB.

3.4.2 Accountability. The capability shall exist to audit all accesses and attempted accesses to objects controlled by the TCB. The TCB shall provide continuous individual accountability through selective auditing (i.e. by providing an audit trail of selectable events) so that actions performed in the system affecting security can be traced to the responsible individual. The capability to select audit events to be recorded is necessary to minimize the expense of auditing and to allow efficient analysis. The data to be audited shall meet the requirements of applicable DOD policy documents for the using agency. A capability shall exist for an authorized agent to access and evaluate accountability information by a secure means within a reasonable time (e.g. one day to do security evaluation of relevant audit data). (REF: paragraph 4.11)

3.4.3 Continuous Protection. The TCB shall be self-protecting to prevent unauthorized on-line changes. All changes to the TCB and attempts to change the TCB (software and firmware portions) shall be audited.

3.5 (B1 level and higher) Operational Level Security Architecture. The system shall be used in a variety of environments which will include all levels of security clearances, varying levels of a need-to-know (e.g. Privacy Act, no foreign, restricted data, etc.), and the full range of configurations possible with the proposed systems and components.

3.6 Security Evaluation and Certification Criteria. The system will be certified for the selected security mode of operation. The DOD Trusted Computer System Evaluation Criteria document shall be an important part of the system security certification and evaluation process. The Government will use this specification and the DOD Trusted Computer System Evaluation Criteria for class C2 and B1 as the basis for the security evaluation and certification criteria for the system. This specification shall be used in cases of conflict with the DOD Trusted Computer System Evaluation Criteria. The establishment of the system's TCB IAW the security requirements is essential to the evaluation process.

3.7 Certification and Accreditation Issues. The Government evaluation authority for class C2 and B1 is the National Computer Security Center

(NCSC). The Government certification authority is the Program Manager or other office designated by the Program Manager.

3.7.1 Contractor Tasks. The Contractor shall perform the following tasks to support the Government in providing a TCB certification for its system. The Accreditation Authority (i.e. Designated Approval Authority (DAA)) will use the Government's analysis of the Contractor's performed tasks or the NCSC evaluation(s) in determining whether the system will be approved for operation. When an NCSC evaluated system(s) is delivered, it must also meet this specification.

3.7.1.1 The CDRL Dxxx deliverables, that are separately orderable, shall follow the DID format (or the commercial equivalent) and be specifically tailored to the Government users' system.

3.7.1.2 The CDRL Fxxx deliverables, that are included with the super-minicomputer operating system, shall follow the DID format (or the commercial equivalent) and be a generic version. For those portions of the deliverable which the Contractor cannot complete because of a lack of specific user related information, the Contractor shall include in its place specific instructions for the user to follow. These instructions should guide the user through the steps required for them to complete those portions of the generic deliverable themselves.

3.7.2 Risk Assessment. The Contractor shall conduct a Risk Analysis and provide a risk assessment (internal) report. (REF: CDRL D001, F001)

3.7.3 System Security Plan. The Contractor shall analyze and develop a plan to accomplish the security requirements for the system. The Government authority will approve the sufficiency of the security approach. (REF: CDRL D002, F002)

3.7.4 System Security Concept of Operations. The Contractor shall develop a system security concept of operations for the proposed system. This document shall address the functional allocation of security requirements to features of the system to include security related aspects of operating positions and fault isolation and correction. Further, it shall include functions such as secure performance of database and software changes. The Government authority will review the system security concept of operations to ensure security control measures are completely and accurately covered. Formal comments shall be coordinated with the program manager for this project. (REF: CDRL D003, F003)

3.7.5 Operations Security\_(OPSEC)\_Plan. The Contractor shall develop preliminary security procedures based on an evaluation of the system security requirements. The Government authority will validate these procedures and evaluate the allocation of security functions between technical enforcement and procedural enforcement. (REF: CDRL D004, F004)

3.7.6 Informal Computer Security Policy Model. A security policy description (security policy model for B1 and higher TCB) shall be developed by the Contractor. The description/model must reflect the system security policy as expressed in this attachment and the security architecture. Review of the description/model will identify systematic definitions of system operation in terms of "subjects," "objects," and their related sensitivity levels. (REF: CDRL D005, F005)

3.7.7 Security Test and Evaluation Master Plans (TEMP) Annex. Contractor developed system security test plans and procedures for hardware, software, firmware, and procedural security controls shall assist in the security evaluation and subsequent certification. The Contractor is tasked to develop system security test procedures. The Government authority will review the system security portions of procedures and system security test procedures and validate their sufficiency for certification. (REF: CDRL D006, F006)

3.7.8 Certification\_Plan. The Contractor shall develop a certification test plan and procedures. A Contractor-developed modular certification test plan and procedures shall assist in system security certification. The Government authority will review the plan to ensure that testing is sufficient for certification. (REF: CDRL D007, F007)

3.7.9 Security Test and Evaluation (ST&E)Test Report. The Contractor shall conduct security tests. All security related sub-systems shall be tested to ensure each operates as specified by the security policy. Prior to system testing of the TCB, it is necessary to ensure each sub-system functions as expected and they properly interface with one another. (REF: CDRL D008, F008)

3.7.10 Certification Report. The Contractor shall conduct independent verification and validation of specific tasks in the areas of the Contractor's system design, specifications development, testing, and implementation. The Contractor shall develop a certification support document that focuses on the act of certifying the communications-computer system. The Government authority will review the Contractor's certification support to validate the adequacy and correctness of those features to satisfy security requirements. This review is a continuing process performed in parallel with TCB design and development. (REF: CDRL D009, F009)

3.7.11 Security Features User's Guide. Provide a security features user's guide to include a checklist to be used by the system security manager when implementing the various levels of protection. Provide one copy with each delivered system. (REF: CDRL D010, F010)

3.7.12 Trusted Facility Manual. Provide a trusted facility manual (TFM) that explains how the system security officer, system administrator, and system operator establish, operate, and maintain a secure system. It shall describe procedures for selecting security options such that the system meets operational requirements in a secure manner. The Government authority will review the manual to validate the adequacy and correctness of those features necessary for the security officer, system administrator, and system operator to maintain system security. Provide one copy with each delivered system. (REF: CDRL D011, F011)

3.7.13 Rating Maintenance Phase (RAMP) Process. The Contractor shall participate in the NCSC RAMP process to reevaluate updates and modifications to its system. Updated, upgraded, and new versions of components shall maintain the evaluated rating from NCSC within a mutually agreeable time frame. (REF: F4.8)

3.7.14 Government's Tasks. The Government's subtasks include:

- a. Conduct a final review of the results of the Contractor's activities and use their input in determining the degree of certification;

b. Ensure that for the hardware, software, and firmware of the system, the following items have been assessed by the Contractor:

- (1) Security capabilities of the TCB;
- (2) Correctness of TCB operations in relation to criteria, herein,
- (3) Security impact of the TCB interfaces to untrusted processes,
- (4) Operation of workstations, in relation to security,
- (5) Security impacts of maintenance routines and diagnostics.

#### 4 Trusted Computing Base Security Requirements.

4.1 TCB Data Processing Capabilities. The TCB shall include within it all data processing capabilities to be provided for protecting information processed and managed by the system. The TCB shall include parts of the operating system and the application software as well as all hardware and firmware providing the security protection specified herein. As such, the TCB shall enforce the operational level requirements as delineated in paragraph 3.

4.2 TCB Implementation. The TCB implementation may span across computer software configuration items and system configuration items. However, in terms of stating required generic capabilities of the TCB, the TCB is to be viewed as a single conceptual entity.

4.3 TCB Requirements Topics. The TCB requirements are organized into the topics listed below. Each of these topics is individually specified in subsequent paragraphs:

- a. Identification of Subjects and Objects;
- b. Sensitivity Labels;
- c. Security in the Management of Interactive Terminals;
- d. Security in the Management of Storage;
- e. Security Rules for Access Controls;
- f. Security in the Management of User Working Environments;
- g. (B1 level and higher) changes in Sensitivity Levels of Objects;
- h. Auditing Functions to Enforce Security;
- i. Security Administrative Functions.

4.4 Identification of Subjects and Objects. The detailed security requirements for the TCB are described in terms of subjects, objects and their

interactions. This involves mapping of named system resources into these categories and defining their relationships.

4.4.1 Definitions and Concepts. The terms subjects and objects are introduced here for use in defining some of the detailed security requirements for the TCB. In particular, the properties of and relationships between these entities are described below.

4.4.1.1 Subject Definitions. A subject is defined as an active entity that can cause information to flow among objects or change the system state. It can take the form of a device, a program being operated (usually called a process), or a generic system terminal user. The use of the term "generic" is to indicate that a terminal user can include any person working at an system terminal, or an external system which is connected to the system, such that its activities are architecturally viewed as occurring at an operational terminal.

4.4.1.2 Object Definition. An object is a passive entity containing information. Access to an object potentially implies access to its contained information. Objects can be hardware resources or software creations; they can be physical resources or logical abstractions; they can be permanent or temporary; or they can be the sensitive information itself.

4.4.1.2.1 Some hardware examples are disks, tapes, terminals, printer or communication services. Objects may also be subdivisions of the above, such as memory blocks, displays, keyboards, or communication channels.

4.4.1.2.2 Some software examples are memory buffers, records, files, programs, pages, segments, directories, or directory trees.

4.4.1.3 Object Security Level Categories. C2 level object security usage shall be categorized as single level. B1 level and higher object security usage shall be categorized into single level and multilevel. The distinction is based on its mandatory security attributes, as follows:

- a. A single level object/device shall be assigned just one security label at any one time, but the assignment can be changed while the system is in operation;
- b. (B1 level and higher) A multilevel object/device can simultaneously hold data objects with different security classification levels.

#### 4.4.2 Requirements.

4.4.2.1 Named resources accessible to the system shall be mapped into subjects and objects.

4.4.2.2 Every object and every subject under control of the TCB shall be provided with a unique identifier.

4.4.2.3 For every subject, the TCB shall be able to determine its type (e.g. nonprivileged, administrator, nonadministrator, or system function) as well as its security access characteristics (i.e. discretionary for C2 level, mandatory and discretionary for B1 level and higher).

4.4.2.4 Only subjects shall be permitted access to objects.

Every attempt by a subject to access a named object shall be controlled by the TCB. The access shall be permitted only when the subject's security characteristics are fully compatible with those of the object, as defined within paragraph 4.8.

4.5 Sensitivity Level. Security requirements, as applied to subjects and objects, include a number of components. The names given to these components, both individually and collectively, are described below; these terms are used to define the requirements specified herein.

#### 4.5.1 Security Components.

4.5.1.1 (B1 level and higher) Security Classification Level. This term establishes hierarchical distinctions. For example, four levels are commonly defined (Unclassified, Confidential, Secret, and Top Secret).

4.5.1.2 (B1 level and higher) Security Compartments/Categories. These synonymous terms apply to nonhierarchical distinctions. Examples of this type of component could be data from certain types of sensors, the performance characteristics of the sensors, certain types of operational or contingency plans, some special handling restrictions (e.g. no foreign), or some types of distribution limitations (e.g. US citizen only). These categories can be in widespread usage (e.g. all DOD), or they can apply more narrowly (e.g. to a particular system or installation).

4.5.1.3 Distribution Restrictors or Enablers. These designators establish which individuals or groups (e.g. by name or office symbol) may be permitted to access the information. These may also be used to prohibit access by individuals or groups.

4.5.1.4 (B1 level and higher) Access Type Restrictors. These designators shall be used to limit the type of access permitted to an object (e.g. access can be restricted to read only or write only).

#### 4.5.2 Collective Designations.

4.5.2.1 Security\_Label. This term includes the totality of all security control components described in paragraph 4.5.1. above.

4.5.2.2 (B1 level and higher) Security Level, Sensitivity Label, and Mandatory Attributes. All of these terms apply collectively to above paragraphs 4.5.1.1. and 4.5.1.2. Security Level applies to the sensitivity of the information itself, an object within which the information resides, or the security clearance assigned to a subject. The sensitivity label is a small data group attached to or associated with the information and its containing object. The label identifies the security level of the information; it also identifies the level of an object and shall indicate the permitted range of classification levels for an object, when appropriate.

4.5.2.3 Discretionary Access Attributes. This term applies collectively to the attributes described above in paragraph 4.5.1.3. (paragraphs 4.5.1.3 and 4.5.1.4. for B1 level and higher). These controls are termed discretionary in the sense that a subject with certain access permission can pass that permission (perhaps indirectly) to another subject. All data objects shall be required to have attached discretionary access limiters; other objects, such as storage containers or communications

channels, are not required to possess discretionary attributes.

4.5.3 (B1 level and higher) Security Label Information Integrity. The TCB shall assure that all security label data assigned to each subject and object is retained and is correctly and reliably associated with its object or subject. It shall also assure that all of the security label data, their associations with the subjects and objects, and the data content of the objects are not altered, deleted or created other than under its control.

4.5.4 (B1 level and higher) Specific System Security Level Range.

4.5.4.1 (B1 level and higher) This system shall provide for eight (8) classification levels.

4.5.4.2 (B1 level and higher) This system shall provide for 29 security compartments.

4.5.4.3 (B1 level and higher) This system shall provide for a minimum of 1000 individuals or groups to be included on the discretionary distribution restrictor/prohibiter lists, as defined in paragraph 4.5.

4.5.5 Subject Security Data.

4.5.5.1 Security Information, as defined in paragraph 4.4.2.3., shall be associated with each subject.

4.5.5.2 Whenever the subject is an operating computer program (i.e. a process), that process shall be directly associated with just one individual user, i.e. the person being served by the process. The subject data influencing access decisions shall contain the personnel security data associated with the individual user. Accountability records regarding subject and object transactions shall also include the user's identification.

4.5.5.3 (B1 level and higher) The security level and other subject data influencing access decisions shall be within the range of personnel security clearances associated with the individual user. Accountability records regarding subject/object transactions shall also include the user's identity label.

4.5.6 (B1 level and higher) Object Security Data Attachment. The sensitivity label shall be securely and reliably connected (logically attached) to its associated object. These labels, their data content, and some of their usage rules, are defined below.

4.5.6.1 (B1 level and higher) Single Level Objects/Devices.

4.5.6.1.1 (B1 level and higher) The sensitivity label for each single level object/device shall contain the range of security levels permitted for that object/device. When the object/device is in use, the label shall also include the currently assigned level; no level shall be assigned outside the range of levels permitted for that object/device.

4.5.6.1.2 (B1 level and higher) When a single level object/device is initially allocated by the TCB to a subject, the subject shall establish, under direct TCB control, the current object/device security label before the object/device can be utilized by the subject (e.g. the printing of files of a given security label on a printer). A reliable

communication mechanism shall be provided for the subject to communicate the object's device's current security label to the TCB. (REF: paragraph 4.9)

4.5.6.1.3 (B1 level and higher) It shall be possible for the subject to alter, under direct TCB control, the current security label of the single level object/device allocated to the subject (e.g. the current security label of a user terminal that is already in use). The subject shall reliably communicate to the TCB the object/device's new security label. Alteration shall be possible at convenient intervals, depending upon how the single level device is used, and shall not compromise sensitive information.

4.5.6.2 (B1 level and higher) Multilevel Objects/Devices.

4.5.6.2.1 (B1 level and higher) The sensitivity label for each multilevel object/device shall contain the range of security levels permitted for that object/device.

4.5.6.2.2 (B1 level and higher) The security levels of data objects exported/imported over a multilevel object/device shall be within the range of allowable security levels assigned to the object/device.

4.5.7 Information Export and Import. The export/import of information shall be controlled by the TCB and shall follow access control rules defined in paragraph 4.8.

4.5.7.1 (B1 level and higher) When information contained in an object is exported from the system, there shall be a means for the TCB to accurately and unambiguously associate the object's sensitivity label with the information being exported.

4.5.7.2 (B1 level and higher) Further requirements for import/export of data objects are dependent on the object security type, as delineated below.

4.5.7.3 Single level Objects.

4.5.7.3.1 Import. The TCB shall be provided a reliable mechanism for communicating with a subject to enable import of a data object. This mechanism shall permit the TCB to determine the object to be employed.

4.5.7.3.2 (B1 level and higher) Import. When a data object is imported by a subject over a single level object, a reliable communications support mechanism shall be provided to enable the TCB in determining the data object's security label. This mechanism shall permit the TCB to determine the current security label of the information to be imported and the single level object to be employed. The TCB shall ensure the sensitivity levels of the subject and object are such that the mandatory security policy is enforced.

4.5.7.3.3 Export. The following procedures shall be supported when a user wishes to export a data object via a single level object.

4.5.7.3.3.1 A subject that is part of the TCB shall assure the object is available and is compatible with the data object. Also, the TCB shall assure any discretionary restrictions on the data object are compatible with any imposed on the object.

4.5.7.3.3.2 (B1 level and higher) A subject that is part

of the TCB shall assure the single level object is available and its range of security levels is compatible with the label on the data object.

4.5.7.3.3.3 If the above conditions are met, the TCB subject (who will have been given explicit privilege to perform this type of action) shall establish the object's discretionary controls to be the same as the data object's.

4.5.7.3.3.4 (B1 level and higher) If the above conditions are met, the TCB subject (who will have been given explicit privilege to perform this type of action) shall establish the single level object's security label to be the same as the data object's.

4.5.7.3.3.5 The export shall then be performed by the subject, who need not be a part of the TCB.

4.5.7.4 (B1 level and higher) Multilevel Objects.

4.5.7.4.1 (B1 level and higher) Import. The sensitivity label of an imported data object over a multilevel object shall be within the range of security labels assigned to the multilevel object. The sensitivity label of an imported data object over a multilevel object shall be trusted by the TCB.

4.5.7.4.2 (B1 level and higher) Export. When a data object is exported a multilevel object (e.g. a storage disk or a control unit used for storing multilevel data), the sensitivity label of the data object shall also be exported by the TCB and shall reside on the same physical medium as the exported data object and shall be in the same form (i.e. machine readable or human readable form). The sensitivity label of the exported data object shall be within the range of security levels assigned to the multilevel object.

4.5.7.4.3 (B1 level and higher) Communication Protocol. When information is imported or exported over a multilevel object (e.g. a communication channel), the discipline used in communicating with the multilevel object (e.g. the protocol multiplexed) shall dynamically provide for the unambiguous pairing between the sensitivity labels and the associated information exported or imported.

4.5.7.5 Labeling Human Readable Output. The system administrator shall be able to specify the printed or displayed classification (sensitivity for B1 level and higher) label that is to be associated with exported information. The TCB shall mark the beginning and end of all human readable, paged, hard copy output with human readable sensitivity labels that properly represent sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human readable, paged hard copy output with human readable sensitivity labels that properly represent the overall sensitivity of the information on the page, including all labels of required discretionary controls. The TCB shall ensure the human readable sensitivity labels accurately represent the current security label of the single level object over which the information is exported.

4.6 Interactive Terminal Security Management.

4.6.1 User Accountability. Every activity within the system (e.g. accessing or printing a file, sending a message) must be accountable to some system user. To enforce accountability, all users must identify themselves to

the system. The identification is performed when the user logs onto the system through an interactive terminal.

4.6.2 Interactive Terminals. Interactive terminals shall be controlled by the TCB. Active terminal users are subjects. The access control rules (a feature which is a part of the TCB) shall be applied to all accesses between active terminal users and objects (REF: paragraph 4.8).

4.6.2.1 Access control rules consist of discretionary access controls.

4.6.2.2 (B1 level and higher) Access control rules consists of mandatory and discretionary access controls.

4.6.3 Information Export/Import. Export/import of information over interactive terminals shall be IAW the rules for export and import of information over single level objects (REF: paragraph 4.5.7).

4.6.4 Identification, Authentication and Accountability.

4.6.4.1 User Identification. In the use of an interactive terminal by a user, the TCB shall require the user to identify him/herself before performing any other actions. The TCB shall authenticate every user identity. The authentication data profile of each user shall include:

- a. The unique user identity (e.g. user name and password);
- b. (B1 level and higher) The user's authorized security clearance;
- c. The user's security pertinent biographical and other data.

4.6.4.2 Terminal Security Label. The security level of the user shall be equal to that of the terminal.

4.6.4.3 (B1 level and higher) Terminal Security Label. A current security label shall be required to be established when a single level terminal is to be used. This label of the terminal shall be reliably established by the TCB during the log-on procedure. During the log-on, the user will inform the TCB of the desired current security label. The TCB shall ensure the requested security label lies within the range allowed for the terminal. The TCB shall also ensure the requested security level lies within the range authorized for the user, as indicated in the user's authentication data profile.

4.6.4.4 Computer Process Security Level. The security level of any computer processes (subjects) created on behalf of an active terminal user shall be equal to the security level of the active terminal user. For auditing purposes the identity of these subjects shall be the same as the active terminal user.

4.6.4.5 (B1 level and higher) Computer Process Security Level. When these subjects access objects, the TCB shall use the security levels of these subjects, supplemented with other information from the authentication data profile of the active terminal user, in order to apply access controls.

4.6.4.6 Authentication Data Protection. Authentication data

profiles shall be protected so they cannot be acquired by unauthorized users. The TCB shall be able to enforce individual accountability by using the unique identification of each active terminal user. The TCB shall also provide the capability of associating this identity with all auditable actions of the active terminal user. (REF: paragraph 4.11)

#### 4.7 Storage Security Management.

4.7.1 Storage Object Type. When a storage object is created, its type shall be established. Whenever an object used for data storage is initially assigned, allocated or reallocated to a subject from the TCB's pool of unused objects, the TCB shall assure the object contains no data for which the subject is not authorized.

4.7.2 Storage Object Security Level. Each storage object shall be considered to be at its assigned single security level.

4.8 Access Control Security Rules. The access control rules define the conditions under which subjects are allowed to access objects within the system. These rules are intended to prevent the compromise of information contained within the system. Hence, the access control mechanisms are considered very critical in preserving the security provided by the system. The TCB shall mediate all accesses between named subjects and objects IAW applicable access control rules.

##### 4.8.1 (B1 level and higher) Mandatory Access Control Rules.

4.8.1.1 (B1 level and higher) Access to an object by a subject shall be mediated in part by the mandatory access control mechanism within the TCB. This mechanism shall be applicable only for objects which are not multilevel. Access controls for multilevel objects are stated separately. (REF: paragraph 4.8.2).

4.8.1.2 (B1 level and higher) The TCB shall apply the mandatory access control mechanism whenever a subject directly accesses an object which is not multilevel.

4.8.1.3 (B1 level and higher) The mandatory access control mechanism shall enforce the two mandatory access control rules stated below for read access and write access.

4.8.1.3.1 (B1 level and higher) Read Access. The TCB shall allow a subject to read an object only if the hierarchical classification level of the subject is higher than or equal to the hierarchical classification level of the object, and the collection of the nonhierarchical security compartments of the subject include the collection of the nonhierarchical security compartment of the object.

4.8.1.3.2 (B1 level and higher) Write Access. A subject shall be allowed to write an object if the subject's hierarchical classification level is lower than or equal to the object's hierarchical classification level and the collection of the object's nonhierarchical security compartment includes the collection of the subject's nonhierarchical security compartments.

##### 4.8.2 (B1 level and higher) Multilevel Objects Access Control Rule.

4.8.2.1 (B1 level and higher) Access to multilevel objects shall be controlled by a multilevel object access control mechanism and this mechanism shall at least enforce the mandatory access control policy of the system. Different access control mechanisms may be required for different kinds of multilevel objects, depending upon the format structure of the sensitivity labels associated with data objects exported or imported over each kind of object.

4.8.2.2 (B1 level and higher) Only the TCB shall be allowed to directly access multilevel objects.

#### 4.8.3 Discretionary Access Control Rules.

4.8.3.1 Access to objects by subjects shall be mediated in part by a discretionary access control mechanism within the TCB.

4.8.3.2 The TCB shall mediate user access to objects based on need-to-know.

4.8.3.3 (B1 level and higher) The need-to-know access restriction shall be further divided into modes which distinguish between users who are allowed to only examine (read) the object, users who are allowed to alter (write) the object during examination, and users who are allowed to only append (write) data to the object without examination.

4.8.3.4 The discretionary access control mechanism shall operate such that a subject shall be allowed access to an object only if the discretionary access enforcement mechanism indicates the subject has been granted the discretionary access permission (i.e. need-to-know).

4.8.3.5 (B1 level and higher) The discretionary access control mechanism shall operate such that a subject shall be allowed access to an object only if mandatory access rules are satisfied and if the discretionary access enforcement mechanism indicates that the subject has been granted the discretionary access permission (i.e. need-to-know).

4.8.3.6 The discretionary access control mechanism (e.g. self/group/public controls, access control lists) shall allow users to specify and control sharing of data objects. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing such permission shall only be assigned by authorized users.

4.9 User Working Environment Security Management. In order not to compromise information it is necessary to properly isolate the working environment of each user. The following requirements shall pertain to all secure working environments:

- a. The TCB shall control the working/processing environment for each active terminal user;
- b. The TCB shall manage the association between an active terminal user and the working environment of the user;
- c. Every working environment shall be mappable onto one or more

subjects and objects;

- d. (B1 level and higher) The security level of the working environment shall be equal to the security level of the active terminal user associated with the working environment and every working environment shall be mappable to only one subject;
- e. The TCB shall have a capability to isolate each working environment (e.g., through the provisions of distinct address space(s));
- f. The TCB shall be able to uniquely identify the working environment of each user;
- g. The TCB shall provide a capability to create a working environment, associate distinct address space(s) to the working environment, and associate a sensitivity label with each subject and object of the working environment;
- h. The TCB shall preserve the integrity of working environments (i.e. by preventing one working environment from interfering with the proper functioning of another);
- i. The TCB shall provide a capability to dissolve a working environment, disassociate address space(s) from the working environment, and remove each subject and object of the working environment;
- j. It shall be possible for the TCB to determine the active terminal user associated with each subject;
- k. Two distinct subjects of the working environments shall be able to communicate with each other depending on the access control rules between subjects and objects. (REF: paragraph 4.8)

4.10 (B1 level and higher) Changes in Object Sensitivity Levels. The TCB shall allow the system administrator to disable objects from use. Requirements for the alteration of sensitivity labels are stated below.

4.10.1 (B1 level and higher) Label Changes. The TCB shall provide a capability that allows a system administrator to change or modify the contents of the sensitivity labels of objects under explicitly defined and carefully controlled conditions:

- a. (B1 level and higher) The range of allowable classification levels for multilevel and single level objects shall be changeable, but only while the objects are disabled from use;
- b. (B1 level and higher) The current security level of a single level terminal shall be changeable whether or not it is in use;
- c. (B1 level and higher) The current security level of other objects shall be changeable only under explicitly defined and carefully controlled conditions.

4.10.2 (B1 level and higher) Label Control. Only a system administrator, under direct TCB control, or the TCB itself shall be capable of

changing an object's sensitivity label.

4.10.3 (B1 level and higher) Label Sensitivity Level. A subject shall be allowed to modify an object's sensitivity level only if the object's before and after hierarchical classification levels are less than or equal to the subject's hierarchical classification level and the object's before and after nonhierarchical compartments are included within the subject's security compartments and the after must dominate the before.

4.10.4 (B1 level and higher) Label Inaccessible During Change. An object whose sensitivity label is to be changed shall remain inaccessible for any usage until the sensitivity label modification is completed.

4.11 Auditing Functions to Enforce Security. A capability shall be provided to allow an authorized agent to access and evaluate audit information by secure means.

4.11.1 Audit Trail. The TCB shall be able to automatically create an audit trail of accesses or attempted accesses to each object and the system itself to maintain and protect it from modification or unauthorized access or destruction.

4.11.2 Audit Data Protection. The TCB shall protect audit data so read access is limited to subjects authorized to examine audit data.

4.11.3 Auditing Functions.

4.11.3.1 Minimally, each audit record shall identify the active terminal user, type of event, success or failure of the event, and time and date of the event. For object access or deletion events, the audit record shall include:

- a. The name of the object;
- b. The object type;
- c. (B1 level and higher) The security level of the object.

4.11.3.2 The system administrator shall be able to selectively audit the actions of any one or more users, or subjects acting on their half, based on individual identity or object security level. As a minimum, the following events shall be audited:

- a. All unsuccessful access attempts to resources;
- b. System faults and restarts;
- c. All actions of system security administrators and operators;
- d. (B1 level and higher) Sensitivity label change actions (successful and unsuccessful);
- e. Diagnostically detected errors;
- f. Modification to users authentication profile;

- g. Use of identification and authentication mechanisms (i.e. all log-ons successful and unsuccessful);
- h. Introduction of objects to subjects (e.g. file open, file close);
- i. Creation and deletion of objects;
- j. User log-off activity;
- k. (B1 level and higher) Changes in users security level;
- l. Any override of human readable output markings;
- m. Other events as needed.

4.11.4 Data Reduction Tools. Data reduction tools assist the system security administrator investigating security problems. The data reduction tools shall present the audited data in a form that is easily accessed and easily understood by humans. The data reduction tools for the audit trail shall be provided to support the following activities:

- a. Accountability of data;
- b. Investigations of suspected security violations;
- c. Retrieval and printing of selected audit records based on range of specified values of some of the item types and some of the audit record types and meaningful comparisons between different type items.

4.12 Security Administrative Functions. The security administrative functions provide necessary capability to manage security aspects of the system.

4.12.1 Security Administrator Support. As a minimum, the following security related system administrator support features shall be provided:

- a. Activate/deactivate optional security audit features;
- b. Determine system configuration (e.g. terminals, peripherals, tape units, printers);
- c. (B1 level and higher) Establish sensitivity labels of objects;
- d. Establish, modify, activate and deactivate access authorizations of users (based on information included in the user's authentication profile);
- e. Enable and disable capabilities to establish user and network connections;
- f. Audit security related activities;
- g. Run security confidence tests for hardware (off-line);
- h. Selectively enable and disable equipment checkout diagnostics;

- i. Allow selective auditing of the actions of one or more users based on individual identity;
- j. (B1 level and higher) Allow selective auditing of the actions of one or more users based on classification levels of the objects being accessed;
- k. (B1 level and higher) Establish and modify a range of allowable security designations that are applicable for multilevel and single level object/devices.

4.12.2 Security Administrator Identification/Authentication. Individual identification and authentication procedures shall be specifically established for system administrators (i.e. the TCB shall be explicitly cognizant about active terminal users which are system administrators).

## 5 Assurance Controls for TCB Development.

This paragraph states explicitly the implementation structure of the TCB, the kinds of controls that must be followed, and the kinds of methodologies that must be used for the development of the TCB. The kinds of assurance factors required for TCB construction (which provide for ease of modification and evaluation, more error free implementation, and less opportunity for the introduction of "Trojan Horses" for the level of trust required in the system) are stated below.

5.1 TCB Design and Testing Control. The methods to be used for designing and testing the TCB shall be as follows.

### 5.1.1 Design Specification and Verification.

5.1.1.1 The TCB design and implementation shall be based on the DOD security policy. The Contractor's design shall be shown to express the DOD security policy.

5.1.1.2 (B1 level and higher) The TCB design and implementation shall be based on an informal or formal model of the DOD security policy. The model shall be shown to express the DOD security policy.

### 5.1.2 TCB Testing and Analysis.

5.1.2.1 The system's security mechanisms shall be tested and found to work as specified herein. This process shall include thorough analysis and testing for detecting violations of all TCB protected resources. A report of the security testing results shall be provided.

5.1.2.2 (B1 level and higher) All discovered design flaws shall be removed or neutralized, and the TCB retested to demonstrate they have been eliminated and new flaws have not been introduced.

5.1.2.3 The Government will thoroughly review of the Contractor's testing of the design, documentation, source code, and object code to uncover all design and implementation flaws that can permit classified data to be compromised, and to assure that no subject (without explicit authorization)

would be able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other subjects.

5.2 Implementation Control. The following constraints shall be adhered to in the development of the TCB.

5.2.1 TCB Domain Constraints. The TCB shall be implemented such that it is protected from external interference or tampering. Specifically, software and firmware, which implement its various functional compartments, shall be confined to domains that are separate from those used for other system functions. This requires hardware features, as well as storage and processing strategies, be employed to isolate data and processing activities within each domain from those in other domains. The establishment of these domains shall be IAW the following:

- a. The domains used for the TCB shall be entirely separate from those used for other system functions;
- b. Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

5.2.2 Software Development Constraints. Current software engineering techniques shall be applied in all phases of system development. Software production shall be consistent with modern engineering practices (e.g. top down structured programming, information hiding, loop free module hierarchy, step-wise refinements, stubs).