DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

1. TITLE	2. IDENTIFICATION NUMBER
TRUSTED FACILITY MANUAL	DI-TMSS-81352

3. DESCRIPTION/PURPOSE

3.1 The Trusted Facility Manual (TFM) explains how the security administrator, system administrator, or operator establish, operate, and maintain a secure environment. The security administrator is responsible for the secure administration of the environment. The system administrator is responsible for the overall functioning of the environment. Finally, the operator is responsible for the day-to-day operation of the environment.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 2.1.3.1.2, 2.1.4.2, 2.2.4.2, 3.1.2.2, 3.1.4.2, 3.2.2.1.1, 3.2.3.1.4, 3.2.4.2, 3.3.2.1.1, 3.3.2.2, 3.3.3.1.4, 3.3.3.1.5, 3.3.4.2 and 4.1.3.2.4 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that requires administrator-oriented documentation as prescribed by DOD-5200.28-STD, Department of Defense Trusted

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6942

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. The TFM shall contain:

a. Cover Sheet. Include Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version, number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Provide sheet delimiting cumulative page changes from previous version(s).

c. Table of Contents. Include paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages, that briefly summarizes the Trusted Facility Manual.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

Block 7. APPLICATION/INTERRELATIONSHIP (Continued)

Computer System Evaluation Criteria, Classes C1 (Discretionary Security Protection), and above, products or their equivalent systems.

7.3 The information required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.3.1, 10.3.2, 10.3.3, 10.3.4, and 10.3.5 is necessary for various classes of products and their equivalent systems.

Block 10. PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Manual.
i. Attachments.
j. Appendices.
k. Bibliography. List reference sources and applicable documents.
l. Subjective Index. An exhaustive index of the key word or theme in each paragraph shall be provided.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.
b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.
c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.
d. Chapters shall begin on an odd-numbered (right hand) page.
e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.
f. Fold out pages shall be kept to a minimum.
g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. The type font shall be standard 10 pitch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or jagged right (left justified only) shall be used.
h. At least one inch margins shall be provided all around to allow for drilling and binding.
i. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.
j. The manual shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 Content. The Trusted Facility Manual (TFM) shall describe procedures for selecting security options that are needed to meet operational requirements in a secure manner. The level of detail should span the gap between the user-oriented Security Features User's Guide and the security engineer-oriented design documentation. The TFM shall be addressed to the system administrator, security administrator, or operator and provide the following information:

a. The TFM shall briefly identify and describe the computer acquisition for which the TFM applies. It shall identify and describe any peripheral equipment necessary for either a secure or functional application. The TFM shall also discuss, if appropriate, use in all possible different environments.

Block 10. PREPARATION INSTRUCTIONS (Continued)

b. The TFM shall describe all of the security mechanisms for the computer environment as these features involve the administrator: the communication (e.g., communications links and network connections); TEMPEST; hardware; software; and storage media.

c. The TFM shall describe the cautions about functions and privileges that should be controlled when running a secure facility.

d. The TFM shall describe the procedures (for hardware and software features) that must be used to periodically validate the correct operation of the on-site operational TCB hardware and firmware elements.

10.3.1 Classes C2 and above products and their equivalent systems. The following shall be included:

a. Identification of the audit files. It shall describe the procedures for examining and maintaining the audit files.

b. Identification of the audited events. It shall describe the detailed audit record structure for each type of audit event.

10.3.2 Classes B1 and above products and their equivalent systems. The following shall be included:

a. A description of the duties, responsibilities, functions, privileges, and interrelationships of the system user, operator, and administrator related to security. This shall include the actions required to change the security characteristics of a user/administrator.

b. The guidelines on the consistent and effective use of the facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner.

c. The guidelines on the consistent and effective use of the protection features (e.g., controlling access, initialization of storage objects, importation of data without labels, label designation of communications channels, exportation of labels, labeling of human-readable output, identification and authentication of users). This shall include how the protection features interact.

d. A description of the procedures used to generate a new TCB. The steps necessary to validate and ensure that all changes which are incorporated conform to the requirements for the TCB class shall be described in the TFM.

e. A description of how the audit mechanism audits the override of human readable output markings.

10.3.3 Classes B2 and above products and their equivalent systems. The following shall be included:

a. The TCB modules that contain the reference validation mechanism shall be identified in the TFM.

b. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described in the TFM.

c. The separation of operator and administrator functions.

d. The procedures that the administrator/user must follow to reach the trusted communication path between the administrator/user and the TCB.

Block 10. PREPARATION INSTRUCTIONS (Continued)

e. The guidelines on the consistent and effective use of the protection features (e.g., change of terminal user security level during interactive session, assignment of security levels to attached devices, identification of covert storage channels in audit data, and safeguards to ensure least privilege). This shall include how the protection features interact.

10.3.4 Classes B3 and above products and their equivalent systems. The following shall be included:

a. Operational procedures necessary to achieve the initial secure processing state. Include any instructions necessary to maintain the secure state.

b. The functions performed in the role of a security administrator shall be identified in the TFM. The TFM shall describe the procedure (a distinct auditable action) that allows a user to access the security administrator role. The TFM shall identify the means by which non-security functions (e.g., those essential to performing the security role effectively) can be performed in the security administration role.

c. The mechanism that monitors the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. The TFM shall describe how the security administrator will be notified when thresholds are exceeded. The TFM shall also identify the security administrator's role in the action which will occur to terminate the events, if the occurrence or accumulation of these security relevant events continues.

d. The procedures for the administrator/user to utilize the trusted communication path between the TCB and the administrator/ user, for use when a positive TCB-to-user connection is required (e.g., login, change subject security level), shall be explicitly defined in the TFM. The TFM shall describe how the communications via this trusted path is activated exclusively by the administrator/user or the TCB. The TFM shall describe how the trusted path is logically isolated and unmistakably distinguishable by the administrator/user from other paths.

e. The guidelines on the consistent and effective use of the protection features (e.g., listing individuals or groups with access to specific objects, and identification of covert channels in audit data). This shall include how the protection features interact.

f. The TFM shall include the description of procedures necessary to resume secure operation after any lapse of operation. The following items shall be included in the TFM to be assigned exclusively to administrative personnel with security-relevant responsibility.

1) Procedures for analysis of dumps, for consistency checking of TCB objects, and for cold start and emergency restart.

2) A description of the types of tolerated failures and examples of the recommended procedures for responding to such failures.

3) Procedures for running periodic integrity checks on the TCB database and for repairing damaged security labels.

4) Procedures for handling inconsistencies of the objects (e.g., duplicate allocation of disk blocks to objects, inconsistent object links).

5)Lists of commands, TCB calls, and function definitions for trusted recovery (whenever these aren't documented in the DTLS).

6) Examples of, and warnings about, potential misuse of trusted recovery procedures.

10.3.5 Classes A1 products and their equivalent systems. The following shall be included:

a. A description of the distribution facility procedures provided for maintaining the integrity of the on-site operational TCB master copy.

b. A description of the procedures that ensure that the TCB software, firmware, and hardware updates distributed are exactly as specified by the master copies.