DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

1. TITLE
DESCRIPTIVE TOP LEVEL SPECIFICATION

2. IDENTIFICATION NUMBER
DI-MISC-81342

3. DESCRIPTION/PURPOSE
3.1 The Descriptive Top Level Specification (DTLS) is a top level specification using English language descriptions. It completely and accurately describes the trusted computing base (TCB) in terms of exceptions, error messages, and effects. The DTLS is an accurate description of the TCB interface.

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 3.2.3.1.1, 3.2.3.2.2, 3.2.4.4, 3.3.3.2.3, and 4.1.3.2.2 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.
7.2 This DID is applicable to any computer acquisition that calls for a DTLS as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Classes B2 (Structured Protection), B3 (Security Domains), or A1 (Verified Design) products and their equivalent systems.   (Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6932

10. PREPARATION INSTRUCTIONS
10.1 <u>Source Document</u>. 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 <u>Format</u>. Document the DTLS as follows:

    a. Cover Sheet. Shall contain 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. Shall contain sheets delimiting cumulative page changes from previous versions.
    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 describes the TCB's security-related capabilities.

(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)

7.3 The information required by 10.3 is 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, and 10.3.3 are necessary for various classes of products and their equivalent systems.

Block 10.   PREPARATION INSTRUCTIONS (Continued)

    g. Introduction.
    h. Body of the specification.
    i. Attachments
    j. Appendices.
    k. Bibliography. List reference sources and applicable documents.
    l. Subjective index

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 ragged 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 specification shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 Content. The DTLS shall describe the security capabilities in functional terms and concepts, and therefore takes the broad form of a "security features functional description." It is traceable to the Formal Security Policy Model. The DTLS shall contain the following items:

    a. A summary of the security policy. This discussion shall be in enough detail to form the background for the following discussions.
    b An overview of the TCB design which describes how the reference monitor concept is implemented, gives an explanation of why the TCB is tamper-resistant, cannot be bypassed, and is correctly implemented.
    c. Description of all TCB functions and features that enforce the security policy. The description shall completely and accurately describe the TCB in terms of exceptions, error messages, and effects, and include:

DI-MISC-81342

Block 10. PREPARATION INSTRUCTIONS (Continued)

       (1) Mandatory access controls.
       (2) Discretionary access controls.
       (3) Security labels associated with subjects and objects.
       (4) Markings applied to external media.
       (5) TCB internal data bases.
       (6) Mapping between physical entities (e.g., users, files) and their logical representations (e.g., subjects, objects).
       (7) Policy rules used by the TCB to grant or deny access by subjects to objects (e.g., a subject's clearance must dominate an object's classification in order to be granted access).

    d. An accurate description of the TCB interface.
    e. A complete description of the user interface.

10.3.1 <u>Classes B3 and A1 products and their equivalent systems</u>. The following shall be included in this section:

    a. A convincing argument shall be presented in the document to show that the DTLS is consistent with the Formal Security Policy Model.
    b. A description of the specific TCB protection mechanisms used to ensure trusted recovery functions. It shall also describe the TCB modules implementing interfaces of trusted recovery.

10.3.2 <u>Class A1 products and their equivalent systems.</u> The DTLS shall include those components of the TCB that are implemented as hardware and/or firmware, if their properties are visible at the TCB interface.