DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

1. TITLE	2. IDENTIFICATION NUMBER
FORMAL TOP LEVEL SPECIFICATION	DI-MISC-81347

3. DESCRIPTION/PURPOSE

3.1 The Formal Top Level Specification (FTLS) is a mathematically precise abstract representation of the trusted computing base (TCB). The FTLS provides an accurate description of the TCB interface in terms of exceptions, error messages and effects. The FTLS includes hardware and firmware elements if their properties are visible at 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 4.1 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 an FTLS as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Class A1 (Verified Design) products and their equivalent systems.

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6937

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. Document the FTLS 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. Shall contain 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 definition. List reference sources and applicable documents.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

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

Block 10. PREPARATION INSTRUCTIONS (Continued)

f. Executive Summary, not to exceed two pages.
g. Introduction.
h. Body of the Report.
i. Attachments.
j. Appendices.
k. Bibliography.
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. 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.

10.3 General. The FTLS document shall contain the formal top level specification, its associated proofs and assurance arguments, and supporting explanations and documentation for the specification, proofs, and assurance arguments.

10.4 Content.

10.4.1 Supporting documentation. The FTLS shall provide background information supporting the specification effort. All of this background information is informal in nature and may be presented in English text, and graphic representation where appropriate. The following items shall be included as part of this information:

a. An overview of the FTLS that explains the approach taken, the structure of the specification, what has been included and excluded in the specification, and how the specification relates to the Formal Security Policy Model.
b. Identification of the portions of the FTLS that are implemented in hardware, software, and in firmware if their properties are visible at the TCB interface.
c. A description of the specification/verification methodology chosen, and why it was selected.
d. An introduction to the specification itself, to include identification of the users, subjects, objects, access modes, security labels, security properties, initial state, and operations that are part of the specification.
e. Identification of the assumptions required by the specification, an explanation as to why they are required, and the consequences of violating the assumptions.
f. A combination of formal and informal techniques (e.g., proofs and assurance arguments) that show that the FTLS is consistent with the Formal Security Policy Model.
g. Identification of the axioms used in the proofs, why these axioms are needed, and how they are justified.

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.4.2 The formal top level specification. The following shall be included in this section:

a. As part of the FTLS document, the specification itself shall be presented in the formal mathematical notation of the specification technique chosen. The specification shall include abstract definitions of the functions the TCB performs and the unified protection mechanism required to satisfy the security policy (TCSEC Section 4.1), to include the following:

(1) Representation of subjects, objects, modes of access, and security labels as they are implemented in the TCB.
(2) Representation of hardware and firmware components of the TCB if their properties are visible at the TCB interface.
(3) The set of security properties enforced by the TCB.
(4) Representation of the initial state of the TCB.
(5) Representations of the operations performed by the TCB, including the effects, exceptions, and error messages for interface operations.
(6) A (possibly empty) set of axioms used in the proofs.

b. The FTLS shall include the abstract definitions of the hardware and firmware mechanisms that are used to support separate execution domains.

10.4.3 Proofs and arguments. this section shall contain, a combination of formal techniques (e.g., where verification tools exist) and informal techniques (e.g., convincing assurance arguments) to demonstrate that the FTLS is consistent with the Formal Security Policy Model.