

# DATA ITEM DESCRIPTION

Form Approved  
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE <b>DESIGN SPECIFICATION</b>	2. IDENTIFICATION NUMBER <b>DI-MCCR-81344</b>
---	--

3. DESCRIPTION/PURPOSE  
**3.1 The Design Specification demonstrates the correct implementation and enforcement of the security policy throughout the trusted computing base (TCB). It shall explain the protection mechanisms of the TCB to the extent that the effect a change may have on the TCB can be evaluated prior to a technical change performed.**

(Continued on Page 2)

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

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 2.1.3.1.1, 2.1.4.4, 2.2.3.1.1, 3.1.3.1.1, 3.1.4.4, 3.2.3.1.1, 3.2.3.1.4, 3.2.4.4, 3.3.3.1.1, 3.3.4.4, and 4.1.4.4 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.**  
**7.2. This DID is applicable to any computer acquisition that calls for a Design Specification as specified by DOD-5200.28 STD, Department of Defense Trusted Computer**

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER <b>G6934</b>
------------------------	----------------------	---------------------------------

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 Design Specification 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 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)

System Evaluation Criteria (TCSEC) for TCB Classes C1 (Discretionary Security Protection), and above, products or their equivalent systems. The Design Specification identifies and describes the TCB and its security features.

7.3 The information required by 10.3 is required for all class products and their equivalent systems applicable to the DDI as a whole. In addition, the information required in 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5 and 10.3.6 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.
- l. Subjective index.
- j. Appendices
- k. Bibliography. List reference sources and applicable documents.

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 may 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 Design Specification shall contain the following items:

a. A statement of the security policy. This description shall be in enough detail to form the background for the design discussions.

b. The Design Specification shall relate the security requirements to the architecture.

c. An explanation of how the security policy is translated into a technical solution through the TCB hardware, software, and firmware.

Block 10, PREPARATION INSTRUCTIONS (Continued)

10.3.1 Classes C1, C2, and B1 products and their equivalent systems. The following shall be included in this section:

- a. Description of how the TCB is modularized (if modular).
- b. Description of all interfaces between the TCB modules (if modular).
- c. Description of how the TCB protects itself from external interference or tampering.
- d. Description of the resources which are controlled by the TCB. These resources may be a defined subset of the subjects and objects.

10.3.2 Classes C2 and B1 products and their equivalent systems. The Design Specification shall describe how the TCB isolates the resources to be protected so that they are subject to the access control and auditing requirements.

10.3.3 Classes B1 products and their equivalent systems. The following shall be included in this section:

- a. Identification and description of the TCB protection mechanisms.
- b. An explanation to show that the TCB protection mechanisms satisfy the model.
- c. Description of how the TCB maintains process isolation through the provision of distinct address spaces under its control.

10.3.4 Classes B2 and above products and their equivalent systems. The following shall be included in this section:

- a. Description of how the TCB is structured to facilitate testing.
- b. Description of the different sets of privileges assigned to differing roles (e.g., users, administrators).
- c. Description of the design techniques involved in restricting covert storage channels.
- d. Description of the interfaces between the TCB modules.
- e. Description of how the TCB complies with additional B2 architecture requirements. The following requirements shall be described:
  - 1) TCB maintenance of a domain for its own execution that protects it from external interference or tampering.
  - 2) TCB maintenance of process isolation through the provision of distinct address spaces under its control.
  - 3) Features in hardware, such as segmentation, used to support logically distinct storage objects with separate attributes (namely: readable, writable).
  - 4) TCB modules structured such that the principle of least privilege is enforced.
  - 5) TCB internally structured into well-defined largely independent modules.
  - 6) Effective use of available hardware by TCB to separate those elements that are protection-critical from those that are not.
- f. Description of the trusted communication path between the TCB and user.

Block 10, PREPARATION INSTRUCTIONS (Continued)

10.3.5 Classes B3 and above products and their equivalent systems. The following shall be included in this section:

a. Description of the design techniques involved in restricting covert timing channels.

b. Description of how the TCB complies with additional B3 architecture requirements. The following requirements shall be described:

1) Complete, conceptually simple protection mechanism with precisely defined semantics. The Design Specification shall describe how this mechanism plays a central role in enforcing the internal structuring of the TCB.

2) Significant use of layering, abstraction, and data hiding by the TCB.

3) Minimization of the complexity of the TCB, excluding the modules that are not protection-critical.

c. The Design Specification shall describe the following for trusted recovery:

1) Anticipated classes of failures and discontinuities of operation handled by trusted recovery, automatically or using administrative procedures.

2) Trusted recovery philosophy (e.g., use of failure-atomicity in the design of TCB primitives, of non-atomic actions which allow recovery).

3) Warnings concerning the 'unanticipated' (i.e., rare) failures that can't be handled in a routine manner.

d. Description of how the specific TCB protection mechanisms used ensuring trusted-recovery functions are available only to administrative users.

10.3.6 Class A1 products and their equivalent systems. The Design Specification shall describe the hardware, software, and firmware mechanisms not dealt with in the FTLS but strictly internal to the TCB (e.g., mapping registers, direct memory access I/O).