DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

1. TITLE	2. IDENTIFICATION NUMBER
SECURITY TEST PLAN	DI-NDTI-81351

3. DESCRIPTION/PURPOSE

3.1 The Security Test Plan outlines the test plans and security objectives for a set of specific security tests to be performed. It provides the test concept, reasons, objectives and requirements to be satisfied, support needed, responsible activities associated with the testing, and analysis techniques to be used. It shall provide the strategy to test the security mechanisms of the trusted computing base (TCB).

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 2.2.3.2.1, 3.1.3.2.1, 3.2.3.2.1, 3.3.3.2.1 and 4.1.3.2.1 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 test documentation for the security features as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), Classes C1 (Discretionary Security

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6941

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 a Security Test Plan 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 version(s).

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 summarizes the Security Test Plan.

(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)

Protection), and above, products or their equivalent systems.

7.3 The Security Test Plan is generally produced to support certification and accreditation.

7.4 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, 10.3.3, 10.3.4, 10.3.5, 10.3.6 and 10.3.7 is necessary for various classes of products and their equivalent systems.

Block 10. PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Plan.
i. Attachments.
j. Appendices.
k. Bibliography. List references and all 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-handed) 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. Use standard 10 inch 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 each page 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 plan shall be provided in standard three ring notebook binders for ease of maintenance.

10.3 Content. The Security Test Plan shall include the method by which testing will be performed to determine whether the TCB works as claimed in the documentation. It shall describe how testing will be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. The Security Test Plan shall include the following:

a. An overview of the TCB that will be tested. It shall briefly describe the security protection mechanism(s).

b. A description of the objectives of the test plan, including the following:

Block 10. PREPARATION INSTRUCTIONS (Continued)

1) A functional description of the security test program.
2) Government and contractor participation roles and responsibilities.
3) Facilities where the testing will be performed.
4) Support requirements for the tests (e.g., communications, equipment, test data, etc).
5) Schedule of when testing will be performed.

c. A list of all tests to be accomplished in the order they are to be performed. The list shall include a test for each security protection function (e.g., unauthorized access to audit data). Each listing shall include the following:

1) Name and brief description of test to be performed.
2) Reason for performing test.
3) Functional requirements which will be tested.
4) Objective to be satisfied by each test, including the pass/fail criteria, baseline, duration, and number of times each test should be performed.
5) Specific test support requirements for each test performed.
6) Start and expected completion dates of each test to be performed.

d. Description of the data reduction and analysis techniques that will be used to interpret the data.

e. An overview of the procedures that will be used to validate the test results.

10.3.1 Class C2 products and their equivalent systems. The Security Test Plan shall include a plan for the search for obvious flaws that would:

a. Allow violation of resource isolation.
b. Permit unauthorized access to the audit or authentication data.

10.3.2 Class B1 products and their equivalent systems. The Security Test Plan shall describe the test program's approach to identify and report flaws so that the flaws may be removed or neutralized. It shall include the approach to retest identified flaws to demonstrate that they have been eliminated. This approach shall include regression testing to ascertain whether new flaws have been introduced when removing the originally discovered flaw.

10.3.3 Class B1 and above products and their equivalent systems. The following shall be included:

a. A description of how the design documentation, source code, and object code will be thoroughly analyzed and tested.
b. The plan for tests to:

1) Uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB.
2) Assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users.

10.3.4 Class B2 products and their equivalent systems. The following shall be included:regression testing to ascertain whether new flaws have been introduced when removing

BLOCK 10. PREPARATION INSTRUCTIONS (Continued)

a. A description of the technique to demonstrate that the TCB is relatively resistant to penetration.

b. A description of the test program's approach to retest identified flaws to demonstrate that they have been corrected. This approach shall include the originally discovered flaw.

10.3.5 Class B2 and B3 products and their equivalent systems. The Security Test Plan shall describe the technique to demonstrate that the TCB implementation is consistent with the Descriptive Top Level Specification.

10.3.6 Class B3 and above products and their equivalent systems. The following shall be included:

a. A description of the technique that will be used to determine that the TCB is resistant to penetration.

b. A description of the approach that will be used to prevent design flaws and limit implementation flaws from being found during the final security testing. This approach shall provide a reasonable confidence that few flaws remain for security testing.

c. The Security Test Plan shall include the following test planning for trusted recovery:

1) Test conditions; i.e., a list of discontinuities of operation that can be generated through administrative interfaces and their effects.

2) Test data, consisting of the following:

a) Environment setup; e.g., the TCB and user-level data structures and objects needed to generate the planned discontinuity.

b) Parameters and commands used by the administrators to generate the discontinuity.

c) Expected outcome; e.g., the type of procedures that are started automatically or manually for handling the generated discontinuity and the effect of those procedures on the TCB state.

3) Coverage analysis; e.g., this includes a list of failures, or classes of failures, whose effect is covered by the generated discontinuities, and a list of spontaneous failures, or classes of failures, whose effect isn't covered by the test.

10.3.7 Class A1 products and their equivalent systems. The following shall be included:

a. A description of the technique to demonstrate that the TCB implementation is consistent with the Formal Top Level Specification (FTLS).

b. A description of how the mapping of the FTLS to the source code may form a basis for penetration testing.